One Hacker

Nº1
1,90 EUROS
Canarias 2,10€
www.onehacker.es

BLACK HACKERS
Pueden controlar tu coche, hundir tu empresa, secuestrar tu PC, manipular un marcapasos...



35
ROBOTS • DRONES • GADGETS STAR WARS • GAFAS VR

1.000.000 DE OFERTAS DE TRABAJO
LAS 20 MEJORES EMPRESAS CÍBER

QUÉ NUBE ELEGIR

¿COMPRAS POR INTERNET?
DIEZ FORMAS EN LAS QUE TE PUEDEN ROBAR

QUÉ TIENEN QUE DECIR ESTOS HACKERS
CHEMA ALONSO, CARLES SOLÉ, ANDRÉS TARASCO, JOSEP ALBORS, ÁNGEL AVILÉS, JULIO VIVERO, JUAN ANTONIO CALLES, DEEPAK DASWANI, RUBÉN SANTAMARTA...

SI UTILIZAS ORDENADOR, MÓVIL, TABLET...

GUÍA PARA PROTEGER TU CIBERVIDA



Grupo Atenea
Seguridad Nacional

SUMARIO

One Hacker


88


28


78



48

Palabra DE HACKER

Ser hacker va más allá de la informática. Se trata de una actitud: la de vivir en constante reto para "dar la vuelta" a los problemas que se nos plantean en el día a día logrando soluciones que nadie ha pensado. Eso es ser hacker. Con ese espírtitu nace One Hacker y a él se suma un amplio equipo de sabios.

El término hacker tiene casi medio siglo de existencia. Nace de las bromas que se gastaban, con códigos de programación, los estudiantes del Massachusetts Institute of Technology –MIT- en los años 60. Unas bromas que llamaban 'hacks' y cuyos creadores eran llamados 'hackers'. Con el tiempo, los más brillantes ingenieros de este centro fundaron el Laboratorio de Inteligencia Artificial del MIT caracterizándose por su entusiasmo por el software libre -creado por gente que lo dona al gran público, sin derechos de propiedad-. Este movimiento fue el impulsor y el creador de lo que hoy llamamos Internet.

Por eso, choca que el diccionario de la Real Academia Española lo define como 'pirata informático', un error que mancha la reputación de los hackers criminalizando su trabajo. De hecho, ningún experto informático reconocerá serlo, ya que sólo los mejores pueden considerarse así. Según el diccionario de los hackers, redactado por Steven Levy, se considera como tal todo individuo que se dedica a programar de forma entusiasta y que pone la información al alcance de todos. A Román Ramírez, presidente de RootedCON -uno de los foros de hackers más conocidos de España-, le gusta recordar que los hackers "son personas con una serie de habilidades de pensamiento lateral y disruptivo". Por ello - recuerda- "un hacker no es necesariamente un informático. Los hay en el espectro financiero, en el jurídico, en la ingeniería, en el arte... simplemente, porque han descubierto una manera 'de retorcer' las cosas para hacer algo para lo que no estaban pensadas". Ser hacker es un orgullo. Y con ese término nos atrevemos a bautizar esta nueva revista de seguridad informática, abierta tanto a los grandes hackers españoles -presentes en foros como RootedCON, Navaja Negra, Conecta, etc- como a las asociaciones más importantes -como el ISMS Forum o el CCI-, a organismos públicos -como el Incibe y el CNPIC- y, por supuesto, a esos dos centenares de empresas de ciberseguridad que nos permiten vivir seguros y disfrutar de una vida digital plena. Todos ellos componen la familia One Hacker. ¿Nos acompañas?

Manifiesto hacker

En 1984, Steven Levy, publicó el libro 'Hackers: heroes of the computer revolution' en el que plasmó, por primera vez, la idea de la ética hacker basada en seis fundamentos:

#1
El acceso a los ordenadores debe ser ilimitado y total.

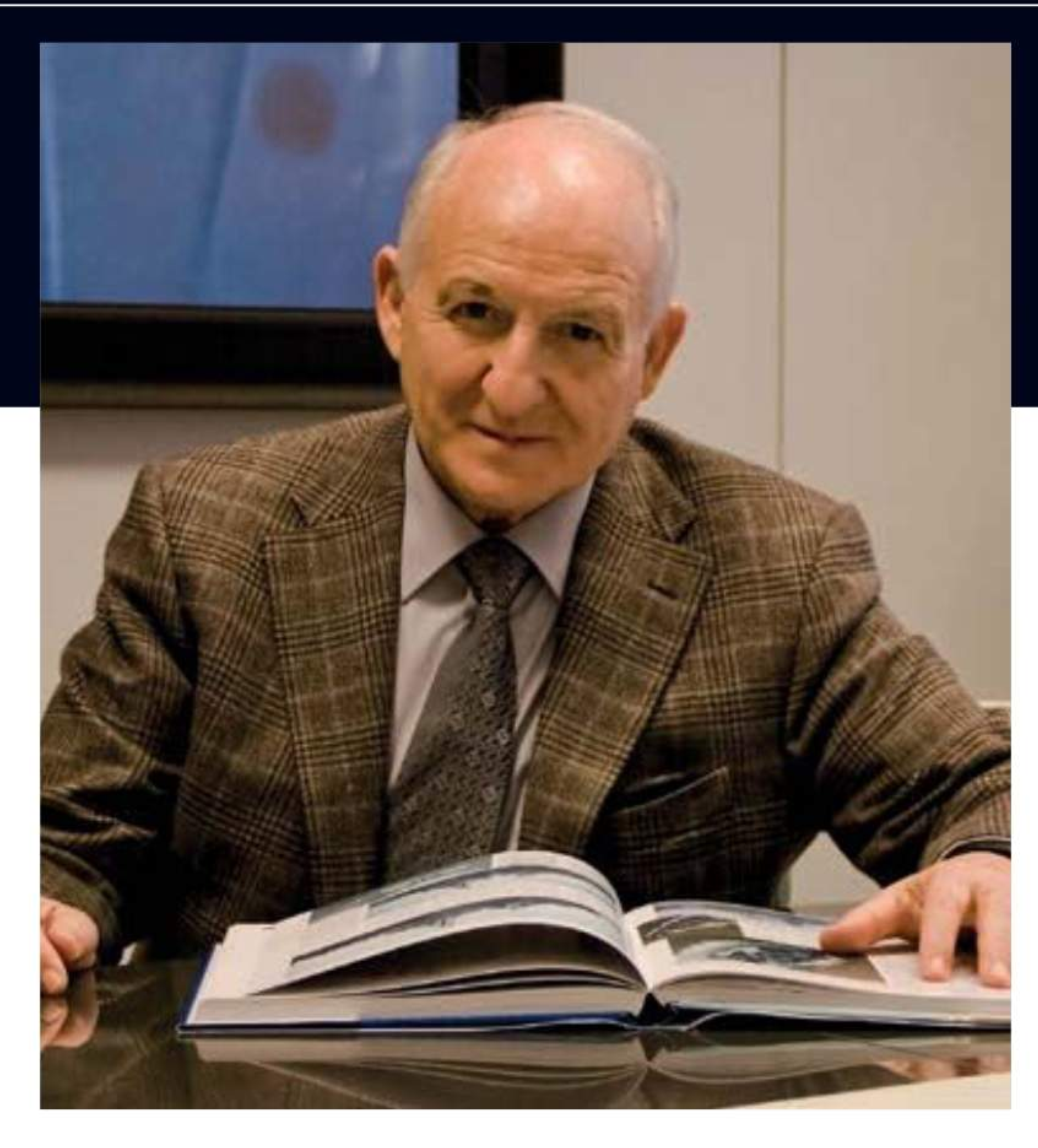
#2
Toda información debe ser libre.

#3
Es necesario promover la descentralización –y desconfiar de los poderes establecidos-.

#4
Los hackers deberían ser juzgados por su labor y no por cosas como su raza, edad o posición social.

#5
Se puede crear arte y belleza en un ordenador.

#6
Los ordenadores pueden cambiar tu vida para mejor.



ES HORA DE ONE HACKER

EN 2020, HABRÁ 20.000 MILLONES DE DISPOSITIVOS INTERCONECTADOS CON LOS QUE INTERACTUAREMOS

Lo 'ciber' es hoy, en esta sociedad tecnológica y global del conocimiento, una dimensión inevitable en nuestro día a día, en la que aspiramos a progresar en libertad y proteger nuestros intereses y privacidad.

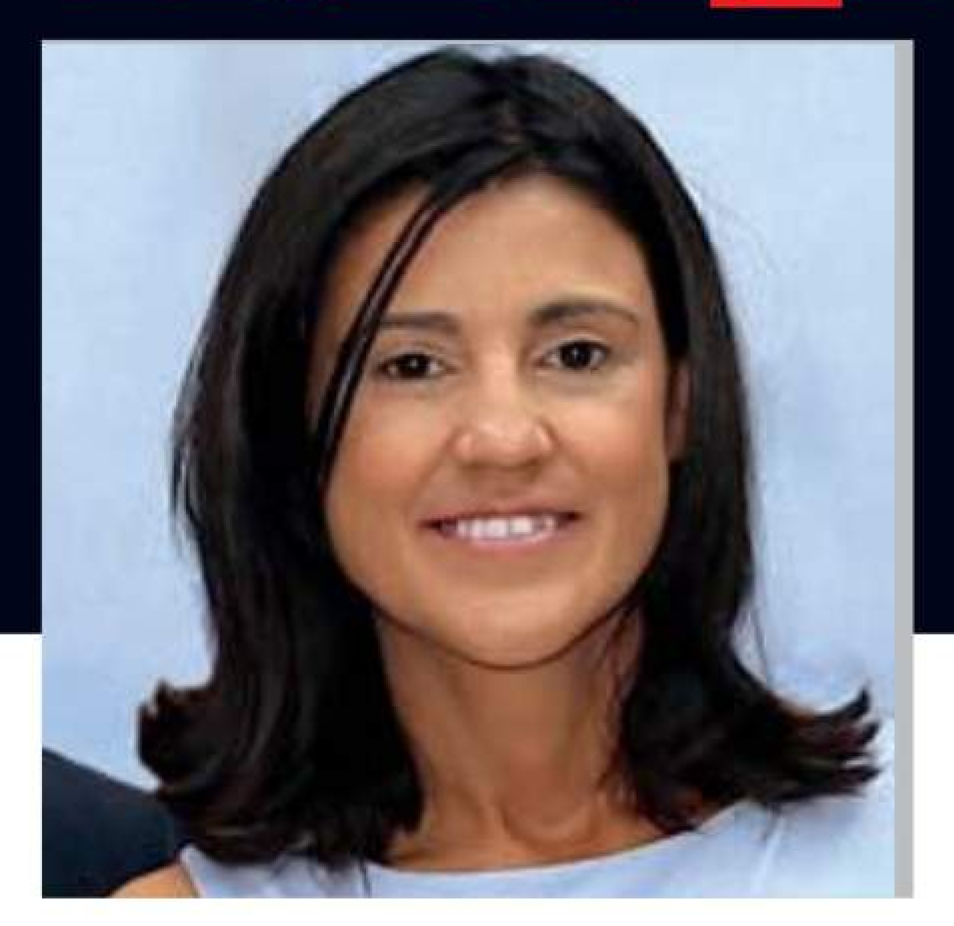
También tiene lo 'ciber' una dimensión social, hasta el punto que cuando delincuentes o enemigos vulneran los sistemas críticos de nuestra nación con ciberataques, puede acarrearnos gravísimos perjuicios a los intereses colectivos y a nuestras actividades personales y laborales.

Por esto, las naciones en su Estrategia de Seguridad Nacional consideran los ciberataques como unas de las más graves amenazas a neutralizar.

ONE Hacker, la revista que desde hoy llega a tus manos, va a informarte, con los asesores más especializados y los mejores hackers, sobre los conocimientos y recomendaciones que más pueden contribuir a que conozcas los riesgos y las soluciones que te protegen a ti y a tu familia, a tu trabajo y a tu empresa.

Con ONE Hacker, además, contribuirás al fomento de una cultura 'ciber' que hoy te es necesaria para ser una persona influyente, de éxito y, como un ciudadano responsable y solidario, poder contribuir a que nuestra sociedad sea más segura.

José Luis Cortina
PRESIDENTE DE GRUPO ATENEA



LA CIBERVIDA...

¿Llevas una doble vida? ¿una convencional y otra que compartes en el ciberespacio? Entonces, te gustará One Hacker. Los mejores hackers de España te cuentan cómo controlar un coche, amañar unas elecciones, estafarte en internet...pero, lo más importante, también te enseñan cómo protegerte de todo ello.

Azucena Hernández
DIRECTORA DE ONE HACKER Y ONE MAGAZINE



¿TE APUNTAS?

One Hacker pretende dar respuesta a las preguntas sobre los riesgos que corres en la red. ¿Nuestro reto? Ser la primera revista que arroje luz sobre la lucha diaria de unos pocos en el ciberespacio para que todos vivamos mejor y más seguro.

José Manuel Vera
DIRECTOR ADJUNTO DE ONE HACKER

Nuestros EXPERTOS



A
Directora
AZUCENA HERNÁNDEZ

B
Director adjunto
JOSÉ MANUEL VERA

C
Redactor jefe
JAVIER GARCÍA

D
Webmaster
SERGIO ÁLVAREZ

E
Jefe de diseño
FERNANDO TEMPRANO

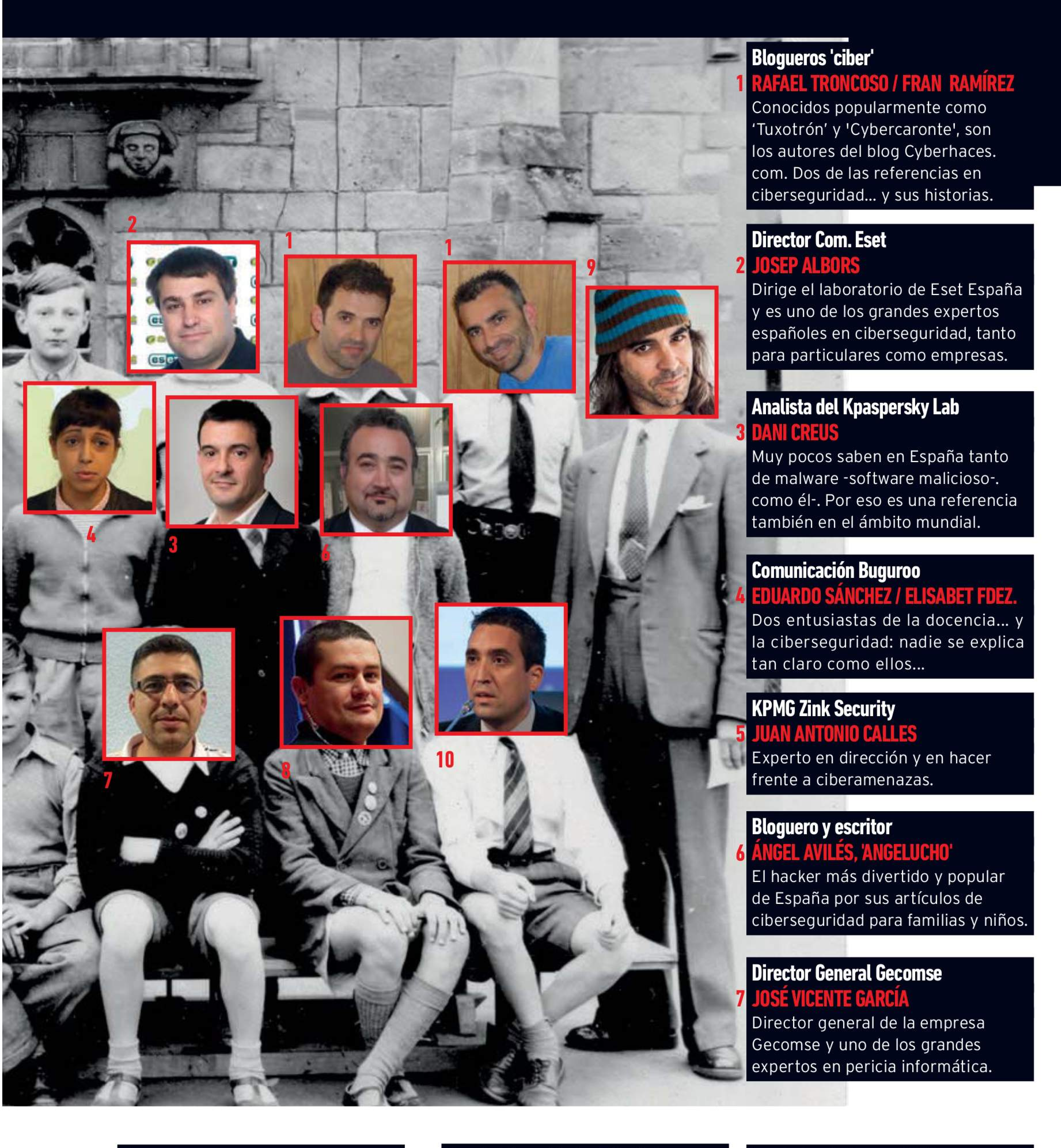
F
Subdirector Técnico
ANTONIO MANZANO

G
Fotógrafa
TERESA BRITO

H
Jefe cíber-internacional
BORJA GARCÍA DE SOLA

I
Diseñadora
LETICIA MACHADO

J
Jefe de cíber-defensa
DAVID NORIEGA



Blogueros 'ciber'
1 **RAFAEL TRONCOSO / FRAN RAMÍREZ**
Conocidos popularmente como 'Tuxotrón' y 'Cybercaronte', son los autores del blog Cyberhaces.com. Dos de las referencias en ciberseguridad... y sus historias.

Director Com. Eset
2 **JOSEP ALBORS**
Dirige el laboratorio de Eset España y es uno de los grandes expertos españoles en ciberseguridad, tanto para particulares como empresas.

Analista del Kpaspersky Lab
3 **DANI CREUS**
Muy pocos saben en España tanto de malware -software malicioso-. como él-. Por eso es una referencia también en el ámbito mundial.

Comunicación Buguroo
4 **EDUARDO SÁNCHEZ / ELISABET FDEZ.**
Dos entusiastas de la docencia... y la ciberseguridad: nadie se explica tan claro como ellos...

KPMG Zink Security
5 **JUAN ANTONIO CALLES**
Experto en dirección y en hacer frente a ciberamenazas.

Bloguero y escritor
6 **ÁNGEL AVILÉS, 'ANGELUCHO'**
El hacker más divertido y popular de España por sus artículos de ciberseguridad para familias y niños.

Director General Gecomse
7 **JOSÉ VICENTE GARCÍA**
Director general de la empresa Gecomse y uno de los grandes expertos en pericia informática.

Grupo de Delitos Telemáticos de la Guardia Civil
10 **ÓSCAR DE LA CRUZ**
Comandante y uno de los grandes responsables de la lucha española contra la ciberdelincuencia.

Ceo de Eleven Paths, Telefónica
9 **CHEMA ALONSO**
Hacker mediático y autor del blog 'El lado del mal'. Responsable de software tan emblemático como Foca o Lacht.

Fundador de RootedCON
8 **ROMÁN RAMIREZ**
Es una referencia en ciberseguridad y el creador del congreso de hackers más importante de España, el RootedCON.

DICCIONARIO HACKER

ADWARE
Programas que, cuando navegas por Internet, te muestra publicidad; bien con ventanas que aparecen de repente o bien mediante banners -espacio insertado en una web-... Esos programas se instalan, a veces, sin que lo sepa el usuario.

ARMOURING
Técnica que utilizan los virus para impedir ser detectados por los antivirus.

AUTOENCRIPTACIÓN
Operación mediante la cual un virus codifica -cifra- parte o la totalidad de su información para dificultar el estudio de su contenido.

ATAQUE AVANZADO PERSISTENTE -APT-
Aquellos cuyo objetivo es una persona, empresa o infraestructura crítica, realizados de forma imperceptible y durante un largo periodo de tiempo. Son los más temidos por los expertos en ciberseguridad, porque sus efectos pueden ser devastadores.

BACKDOOR
O 'puerta trasera'; se trata del lugar 'virtual' que crea un programa en nuestro ordenador para entrar y salir de nuestro sistema sin permiso del usuario y sin ser detectado.

BOMBA LÓGICA
Es un programa de apariencia inofensiva, que puede provocar acciones dañinas en tu ordenador, al igual que cualquier otro virus.

BOT
Es la contracción de 'robot'. Programa que permite controlar un sistema 'de forma remota' -a distancia- sin el conocimiento del usuario.

BOTNET RED
Grupo de ordenadores controlados a distancia por un hacker: con ellos se puede enviar, en un instante, millones de correos a una o varias empresas... y bloquear sus servidores.

CAVITY
Técnica utilizada por algunos virus y 'gusanos informáticos' para dificultar su localización.

CERT
Es un centro de respuestas a incidentes de seguridad en tecnologías informáticas.

CIBERARMA
Programa informático utilizado por las unidades militares para anular un ataque o inutilizar un sistema. A diferencia de las armas convencionales, de momento, no hay ninguna regulación sobre ellas.

CONDICIÓN DE ACTIVACIÓN -TRIGGER-
Son las condiciones bajo las cuales un virus se activa o comienza a llevar a cabo sus acciones dentro el ordenador infectado.

CRIMEWARE
Todo aquel programa, mensaje o documento utilizado para obtener beneficios económicos de forma fraudulenta.

DIALER
Es un programa que suele ser utilizado para redirigir, de forma maliciosa y sin que el usuario lo sepa, las conexiones mientras se navega por Internet. Su objetivo es 'cerrar' la conexión telefónica que se está utilizando en ese momento y establecer otra, marcando un número de teléfono de tarificación especial. Esto supondrá un notable aumento del importe en la factura telefónica para el usuario afectado.

DOS
Ataque de un software malicioso que impide que podamos usar o acceder a ciertos servicios -del sistema operativo, de servidores web, etc- desde nuestro ordenador. Son los ataques más empleados contra todo tipo de organismos y empresas, sobre todo financieras.

DROPPER
Es un fichero ejecutable en el ordenador y que contiene varios tipos de virus en su interior.

EICAR
Siglas de European Institute of Computer Anti-Virus Research, organismo que ha creado un método para evaluar la fiabilidad de los sistemas antivirus.

EPO
Siglas de Entry Point Obscuring; es una técnica para infectar programas con un virus que oculta su punto de entrada para evitar ser detectado. El virus, en lugar de actuar al principio del programa, permanece 'latente', permitiendo el correcto funcionamiento de éste hasta el momento en que comienza a actuar.

EXPLOIT
Es una técnica o un programa que aprovecha un fallo de seguridad -lo que se llama una 'vulnerabilidad'- en un protocolo de comunicaciones, sistema operativo, etc... para entrar en él y atacarlo.

FIREWALL
En español, cortafuegos. Es un tipo de software que permite establecer una barrera de protección para salvaguardar un sistema frente a posibles amenazas.

HACKER
Persona con altos conocimientos en seguridad y en informática que le permiten acceder a ordenadores y sistemas evitando todas sus barreras.

BUG, ZERO DAY, MALWARE... SON PALABRAS QUE TODOS EMPLEAN EN EL MUNDO CÍBER. SI NO ERES UN EXPERTO, ESTOS SON LOS TÉRMINOS BÁSICOS QUE DEBES CONOCER.

HIJACKER
Término que significa, literalmente, 'secuestrador'. Es cualquier programa que cambia la configuración del navegador, para que cuando nos conectamos a Internet, la página de inicio o el buscador que normalmente utilizamos 'apunte' a otro sitio distinto del indicado por el usuario.

HOAX
Bulo que se remite por Internet a miles de usuarios. En muchos casos, además, va acompañado de algún software malicioso que lo que hace es que, cuando reenviamos ese mensaje a todos nuestros contactos -las llamadas 'cadenas' de email-, los hackers 'capturan' todas las direcciones a las que lo enviamos.

LADRÓN DE CONTRASEÑAS
Programa que obtiene y guarda datos confidenciales, como las contraseñas de acceso de un usuario -utilizando keyloggers u otros medios-. Dicho programa es capaz de hacer pública esta información, permitiendo que terceras personas puedan utilizarla en perjuicio del usuario afectado.

LAMMER
Persona falta de habilidades técnicas y sociales, o de madurez, que lo hacen un incompetente. Tambien es quien alardea de conocimentos que no tiene.

MALWARE
También conocido como software malicioso, es cualquier programa, documento o mensaje, susceptible de causar perjuicios a los usuarios de sistemas informáticos.

MÉTODO DE INFECCIÓN
Es una de las características más importantes de un virus. Se trata de cada una de las operaciones que el virus realiza para llevar a cabo su infección en el ordenador.

NUKE
Es un tipo de ataque que provoca la caída o pérdida de la conexión de red, causada de forma intencionada por alguna persona. El ordenador sobre el que se realiza un nuke, además, puede quedar bloqueado.

STEALTH
En español, 'ocultación'. Es la técnica utilizada por algunos virus para intentar pasar desapercibidos a los ojos del usuario afectado e, incluso, de algunos antivirus -de forma temporal-.

PARCHE DE SEGURIDAD
Conjunto de ficheros adicionales al software original de una herramienta o programa informático, que sirven para solucionar sus posibles carencias, vulnerabilidades, o defectos de funcionamiento.

PAYLOAD
Son los efectos maliciosos producidos por un virus.

PHISHING
Consiste en el envío masivo a miles de usuarios de mensajes o páginas web; estos adoptan una apariencia 'amigable' para que el usario crea que provienen de una fuente segura, y de esta forma les facilitemos los datos o información que nos solicitan... y con los que nos timarán o estafarán.

RANSOMWARE
Se trata de un malware -programa malicioso- que secuestra tu ordenador para que no pueda funcionar y que, a cambio de su rescate y liberación, te pide una cantidad económica.

SPAM
Es correo electrónico no solicitado, normalmente con contenido publicitario -es decir, más molesto que peligroso-, que se envía de forma masiva a millones de usuarios.

SPYWARE
Son aquellos programas espía que recopilan datos sobre los hábitos de navegación, preferencias y gustos del usuario que navega por Internet.

TROYANO
Programa aparentemente inofensivo que se instala en un ordenador y que permite a un hacker realizar acciones sin el consentimiento del propietario del sistema.

VIRUS DE COMPAÑÍA
Se trata de un tipo de virus que no se incluye dentro de otros programas, sino que se asocia a ellos.

VIRUS INFORMÁTICO
Son programas que se pueden introducir en los ordenadores -también teléfonos móviles o tablets- y sistemas informáticos de formas muy diversas, produciendo efectos molestos, nocivos e incluso destructivos e irreparables.

VIRUS RESIDENTE
Se denomina de esta forma a aquel fichero o programa que se 'implanta', de forma permanente, en la memoria del ordenador, controlando las operaciones realizadas en el sistema.

VULNERABILIDADES
Fallos o 'huecos' de seguridad detectados en algún programa y que aprovechan los virus para acceder a nuestro ordenador.

ZERO DAY
Vulnerabilidad de un programa o sistema informático que nadie conoce, salvo quien la descubre. Hay empresas e incluso cibercriminales que llegan a pagar por ellas hasta medio millón de euros.

CAE EL 'AL CAPONE' DEL CIBERCRIMEN

El georgiano, Gery Shalon, capitaneaba una banda que robaba información privilegiada y manipulaba los precios de las acciones.

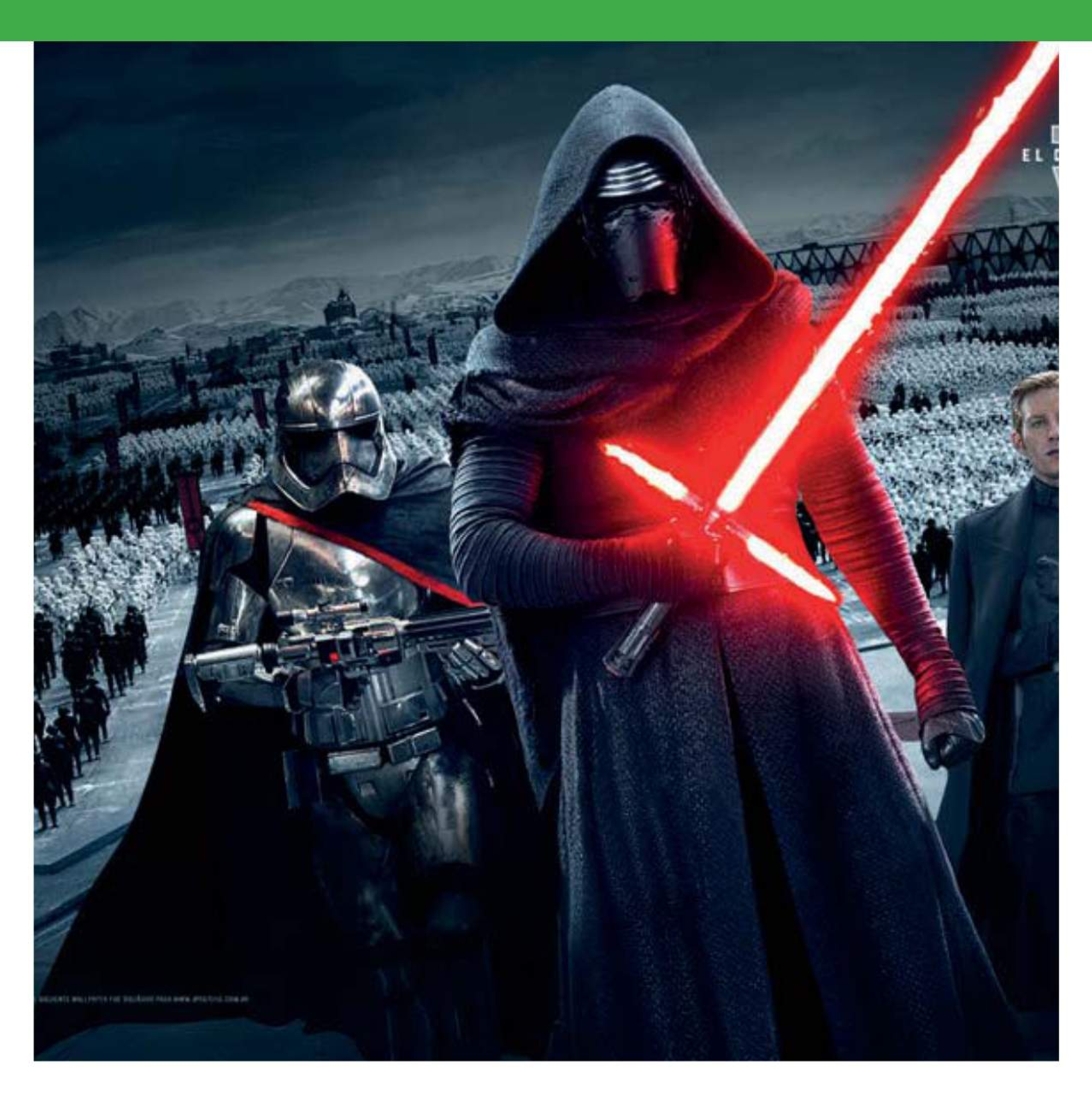
Texto D. Noriega

Alphonse Gabriel Capone, conocido por su segundo apellido, es considerado el gánster más famoso de la historia -a pesar de que en su tarjeta de visita figuraba como vendedor de antigüedades-. Curiosamente, fue detenido y encarcelado por evasión de impuestos, y no por robo, extorsión, chantaje, etc. Negocios criminales que responden a los mismos patrones que las organizaciones criminales que se mueven en el ciberespacio persiguiendo los mismos objetivos. En noviembre, los responsables policiales de EE.UU. han conseguido poner fin al que ha sido considerado el mayor sindicato cibercriminal del país, con la detención de un centenar de personas en unos 50 países y de su líder, el georgiano Gery Shalon, catalogado como el Al Capone del cibercrimen. Esta organización había conseguido, desde 2007, millones de euros de beneficios a costa de todo tipo de 'negocios': desde robar información privilegiada de los principales bancos de inversión hasta extorsionar a casinos online… y, sobre todo, lanzando ciberataques contra los principales inversores de Wall Street.



Shalon llevaba eludiendo la justicia desde hace medio lustro, utilizando identidades falsas -Garri Shalelashvili, Philllipe Mousset o Christopher Engeha-, pasaportes falsos y cuentas encubiertas para evitar ser identificado. Entre otros delitos ha sido acusado de robar información de más de 100 millones de cuentas de clientes de entidades financieras -de las cuales unos 80 pertenecían al banco de inversión JP Morgan-.

Además, la banda era especialista en alterar el precio de las acciones de las empresas, introduciéndose en sus servidores y lanzando noticias sobre ellas que influyesen en los mercados bursátiles y realizando operaciones financieras cuando se hicieran públicas. Por ejemplo, en 2012 manipularon la información de la compañía minera Mustang Alliances: la banda ganó 1,8 millones de euros en bolsa tras inflar un 65 % el precio de las acciones de esta empresa, lanzando una información falsa de que la compañía había encontrado un yacimiento de oro por valor de 1.600 millones. En total, se les acusa de haber obtenido, por métodos criminales, más de 93 millones de euros, que han sido localizados en diversas cuentas bancarias en Suiza.

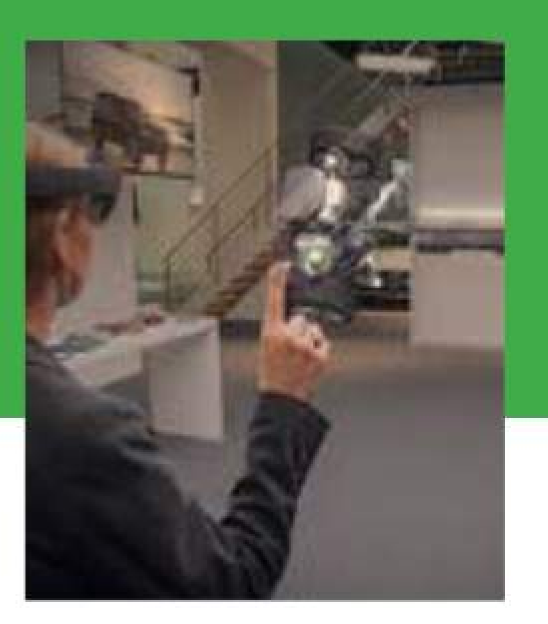


PROGRAMA CON STAR WARS

Una iniciativa en Internet recurre a los personajes de la saga para enseñarte a programar tu propio videojuego, con ayuda del software JavaScript.

Texto S. Lauja

La productora Disney Lucas Film -propietaria de la serie de películas de 'Star Wars'- y la web code.org han presentado una iniciativa mediante la que los aficionados a la saga pueden aprender a programar de la mano de sus personajes preferidos. La idea consiste en una guía mediante la cual, durante una hora, aprenderás los procesos más básicos de la programación informática. El manual se compone de dos bloques: el primero está dedicado a la programación con el software JavaScript, mientras que en el segundo, una vez hayas aprendido a usar dicho programa informático, podrás crear tu propio videojuego aprovechando las capacidades de tu navegador. En el tutorial tendrás que arrastrar las piezas de código correctas para resolver los problemas que se te vayan presentando. Esta iniciativa forma parte de la llamada 'Hora del Código' que tiene en marcha la citada web con el fin de divulgar al gran público conocimientos de programación como los que han servido para crear los efectos especiales de la película que se estrena el 18 de diciembre. **+ Info: code.org/starwars**



ELIGE TU VOLVO CON AYUDA DE LAS GAFAS HOLOLENS

La marca sueca se ha aliado con la multinacional tecnológica Microsoft para crear un configurador de vehículos que utiliza la realidad virtual.

La firma automovilística Volvo permitirá que sus clientes configuren al detalle su futuro coche viéndolo en directo, pero... sin tenerlo físicamente delante. Con ayuda de unas gafas HoloLens de realidad combinada, el comprador se sentará en el concesionario y verá, a través de ellas, un holograma del coche, sobre el que podrá ir cambiando el color de la carrocería, las llantas y otros elementos de diseño. "La realidad aumentada nos da la oportunidad de meternos en la piel del vehículo", ha afirmado Thomas Andersson, vicepresidente de marketing global de Volvo Car Group.



CUIDADO CON ESTOS BULOS

Si recibes un mensaje como éste, es que te intentan robar

"Estimado cliente de Amazon: por favor, asegúrese de que sus datos son los correctos. Como parte de nuestros esfuerzos por proporcionarle seguridad, regularmente supervisamos las cuentas de nuestros clientes. Por favor, su cuenta ha sido suspendida y necesitamos verificar sus datos". Este es el correo electrónico que han recibido en los últimos meses algunos internautas pero... ¿qué dice el Grupo de Delitos Telemáticos de la Guardia Civil? Esto: "¡OJO! Es un Phishing, es decir, si les haces caso te 'roban' la identidad y pueden acceder a tus datos y contraseñas a través del ordenador". Ninguna empresa ni entidad bancaria te pedirá información confidencial -como contraseñas o cuentas bancarias- mediante un email.

CIBER GUERRA 2020

Entre las propuestas de Defensa presentadas por el Congreso de EE.UU. al presidente Obama, figura la práctica de 'cibermaniobras' con un realismo increíble.

Texto: S. Álvarez

Los legisladores estadounidenses son conscientes de que las guerras del futuro se librarán en el ciberespacio. Para que EE.UU. esté preparado contra los ciberataques de sus adversarios más poderosos, el Congreso ha elaborado la Ley de Autorización de Defensa Nacional 2016 -la '2016 National Defense Authorization Act', en inglés-. Esta ley, encarga al Mando de Ciberdefensa la realización de 'cibermaniobras', que tendrán que simular ataques informáticos como los que, según las previsiones de EE.UU., podrían estar en condiciones de realizar Rusia, China, Irán y Corea del Norte, entre los años 2020 y 2025. La preocupación de los legisladores de EE.UU. no es para menos: en junio, el Director de Inteligencia Nacional, James Clapper, declaró que China es el "principal sospechoso" de haber robado datos sobre 21,5 millones de personas a la Oficina de Gestión del Personal del Gobierno Federal. Además, advirtió de que Rusia estaría trabajando en formas de hacerse con el control de infraestructuras críticas. La Ley de Autorización de Defensa Nacional 2016 ha recibido el visto bueno del Pentágono, pero el presidente Barack Obama ha anunciado que la vetará en su totalidad cuando llegue a su despacho. El portavoz de la Casa Blanca, Josh Earnest, la ha descrito -sin hacer referencia concreta a la parte de ciberguerra- como una "manera irresponsable de financiar nuestras prioridades de defensa nacional".



LOS AYUNTAMIENTOS ESTÁN DESPROTEGIDOS

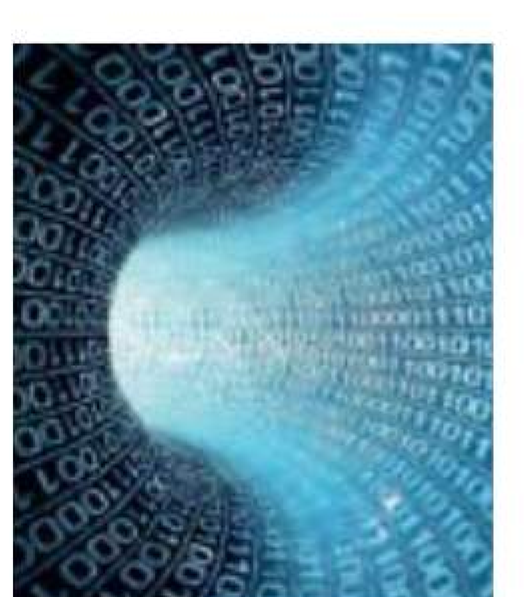
LOS PORTALES DE INTERNET DE NUEVE DE CADA DIEZ CONSISTORIOS ESPAÑOLES TIENEN FALLOS DE SEGURIDAD

La empresa de ciberseguridad Sophos, en colaboración con la compañía de proyectos de seguridad informática Securízame y el despacho de abogados especializados en protección de la información Abanlex, ha presentado un informe en el que señalan que, tras analizar las medidas de seguridad que se aplican en las webs de 77 ayuntamientos españoles, la gran mayoría de ellos -sobre todo los más pequeños- sería un blanco fácil para los cibercriminales. Ante esta situación, un 'black hacker' podría hacerse con los datos personales o cualquier información de los ciudadanos e, incluso, interceptar las comunicaciones para manipularlas. Por ejemplo, los expertos de Sophos detectaron que un 40% de los ayuntamientos sigue soportando el protocolo SSL v2, especialmente vulnerable al tener un algoritmo de cifrado fácil de romper.



LOS HACKERS PROTEGEN A LA REINA ISABEL II

42 de los mejores hackers británicos participaron el 20 de noviembre en el evento 'Cyber Security Challenge UK 2015'. Allí, hicieron un simulacro en el que debían truncar los planes de unos ciberterroristas, que querían acceder al sistema de control ambiental del Palacio de Westminster para atentar contra la Familia Real con ántrax y ébola.



A LAS EMPRESAS ESPAÑOLAS LES CUESTA CREER EN EL BIG DATA

Cerca de un 40% de las empresas españolas no tienen ningún proyecto de Big Data, según la agencia Wunderman. Entre las causas de que haya tantas compañías que no apuesten por el análisis de grandes cantidades de datos están la falta de presupuesto, el desconocimiento y la no identificación del retorno sobre la inversión.



TODOS LOS DATOS DE LA UE, EN UNA SOLA BASE

EL PORTAL EUROPEO DE DATOS PERMITE A UN USUARIO O EMPRESA BUSCAR INFORMACIÓN PUBLICADA POR CUALQUIER ADMINISTRACIÓN EUROPEA

Garantizar el acceso libre a la información es una de las prioridades de la Comisión Europea -CE- para garantizar el buen funcionamiento del mercado digital único, para lo que ha creado el Portal Europeo de Datos. Esta iniciativa ha servido para compilar en una sola base los datos publicados por las administraciones de todos los países de la UE y algunos países vecinos. Así, más de 240.000 conjuntos de datos de 34 países europeos se encuentran ya almacenados en este portal. Cualquier ciudadano de la UE puede consultar el Portal Europeo de Datos: usuarios, empresas, desarrolladores, periodistas... El sitio contiene datos sobre 13 categorías distintas: agricultura, energía, transporte, economía, medio ambiente, educación, salud, ciencia... son algunos de los campos que comprende.



CISCO SYSTEMS REFUERZA SU APUESTA POR EL MUNDO DE LAS VIDEO-CONFERENCIAS

CON EL ANUNCIO DE LA ADQUISICIÓN DE LA EMPRESA ACANO, CISCO DESEMBARCARÁ EN EL MERCADO DEL SOFTWARE COLABORATIVO

La empresa estadounidense Cisco Systems, una compañía especializada en tecnología para videoconferencias, ha invertido 660 millones de euros en esta adquisición. Con ella, busca ofrecer a sus clientes la posibilidad de realizar videoconferencias desde cualquier lugar. De ahí que haya mostrado un gran interés en el software de Acano, con el que es posible conectar audio y vídeo de varios usuarios a través de la nube.

SERVICIOS DE SEGURIDAD

¿SABÍAS QUE CADA SEGUNDO Y MEDIO SE PRODUCE UN **CIBERATAQUE** EN EL MUNDO?

Prosegur responde ante **cualquier amenaza que pueda afectar a sus clientes** con **Servicios de Ciberseguridad** mediante diferentes soluciones:

- Centros de Operaciones (SOC) que permiten dar respuesta a incidencias en modalidad 24x7x365.
- Capacidad de Análisis y Respuesta a información relevante en el ciberespacio.
- Un equipo altamente especializado capaz de resolver cualquier tipo de ciberataque (phishing, malware y botnets entre otros).

Para fomentar la prevención y la detección de este tipo de ataques, Prosegur le ofrece:

 Gestión de vulnerabilidades

 Seguridad en aplicaciones

 Ciberinteligencia

 Monitorización y Correlación (a través de nuestros socs)

 Vigilancia digital

 Administración y operación de infraestructura de seguridad

 twitter.com/prosegur

 linkedin.com/company/prosegur



www.prosegur.com

FLASH, EL SOFTWARE MÁS EXPUESTO

EL INFORME DE INTELIGENCIA SOBRE AMENAZAS GLOBALES 2015 SEÑALA QUE FLASH CONCENTRA LA MAYOR CANTIDAD DE RIESGOS

Internet Explorer, Java y Flash son los tres programas más vulnerables ante los ciberdelincuentes, según el Informe sobre Amenazas Globales de Inteligencia elaborado por la empresa NTT Group. Así, Java presentó un 28% de vulnerabilidades aprovechadas por los cibercriminales, Flash un 26% e Internet Explorer, un 17%. Les siguen el sistema operativo Windows -14 %-, Silverlight -6 %- y Acrobat -4 %-. Además, NTT Group ha constatado que el 74 % de las organizaciones no tenía planes de respuesta a los incidentes.



LA PIEDRA PROTECTORA

El dispositivo Dojo alerta al dueño de la casa de cualquier intrusión en los aparatos de su hogar a través del Internet de las Cosas.

Texto B. García de Sola

Cada vez más dispositivos del hogar podrán conectarse al Internet de las Cosas, todo un campo por explorar en materia de ciberseguridad. Por eso, la empresa Dojo Labs ha lanzado Dojo, uno de los primeros productos pensados para proteger nuestro hogar de los ciberdelincuentes: se trata de un dispositivo marrón con forma de piedra que se conecta al router del domicilio y detecta cualquier intento de intromisión por parte de un ciberdelincuente. Cuando detecta una intrusión -por ejemplo, un intento de manipular la alarma de la casa-, envía una notificación al teléfono móvil de su propietario -para lo que deberás instalar una aplicación con la que conectar también tu teléfono a este dispositivo-, y el color de su carcasa cambia de marrón a naranja. Si es necesario, Dojo bloqueará la amenaza e incluso desconectará de la red el aparato en peligro. El procesador está conectado directamente al router para analizar todo el tráfico de datos y detectar anomalías. Además, gracias a su conexion a la nube, puede tomar nota de los incidentes sufridos por otros usuarios en sus casas. Ya se puede reservar por un precio promocional de 93 euros. **www.dojo-labs.com**

OCIO HACKER

¿QUIERES CONVERTIRTE EN UN EXPERTO? EMPIEZA CON ESTOS TÍTULOS.

// Texto: P. Izquierdo

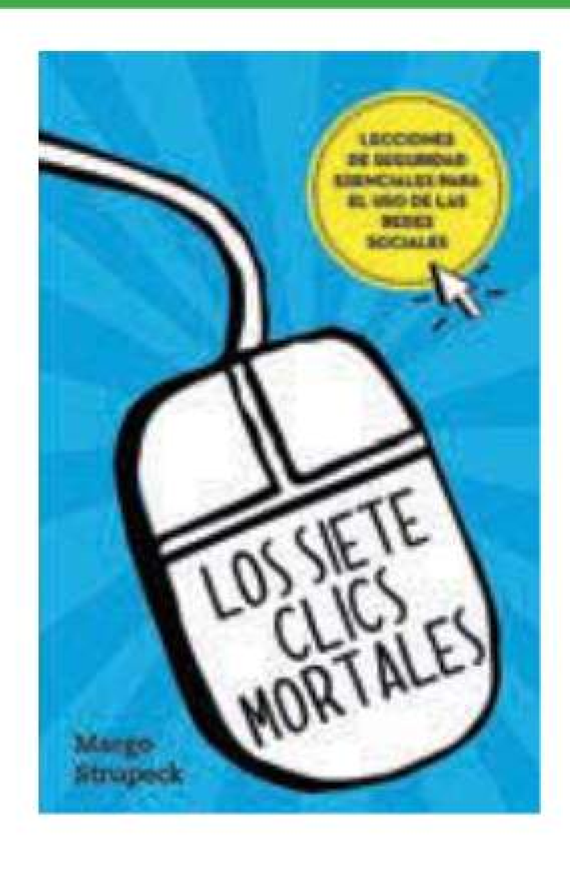


El quinto elemento

Alejandro Suárez,

Deusto • 17,95 €

Un libro de referencia para conocer el trasfondo internacional de la influencia de un hacker en los últimos años: espionaje diplomático, competencia empresarial, ciberterrorismo, robo de secretos militares, sabotaje industrial, márketing, publicidad... Su autor, Alejandro Suárez, lo tiene claro: "La Tercera Guerra Mundial ha comenzado, y todos somos soldados en sus trincheras".

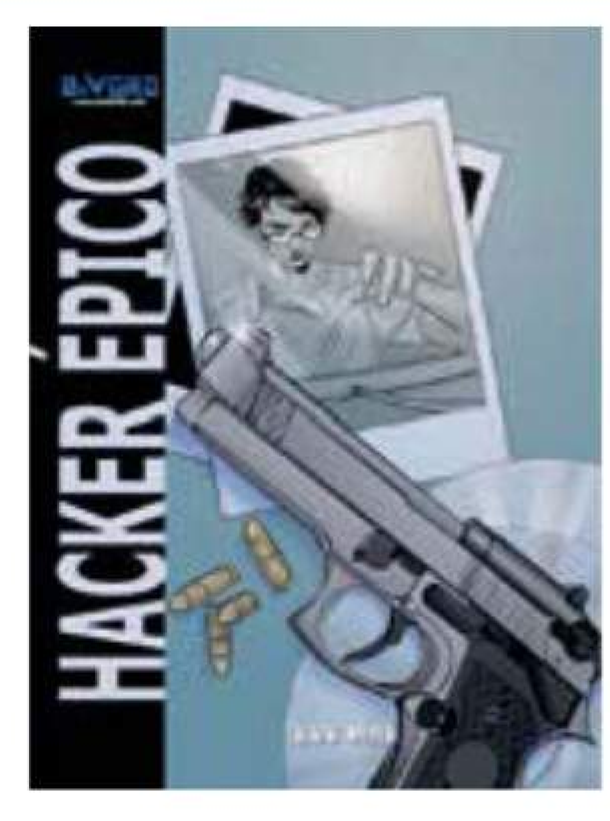


Los siete clics mortales

JAVIER LÓPEZ ALEGRÍA

Altea • 8,53€

Las nuevas tecnologías adquieren mayor protagonismo en nuestra rutina día tras día. Aunque son muchas las ventajas que nos aportan-anonimato, inmediatez, aceleración de los procesos- albergan una gran cantidad de situaciones de riesgo. Este libro contiene información práctica para evitar estas 'trampas digitales' y, también, para solucionar problemas de forma segura. Ofrece consejos sobre temas como el acoso cibernético y el robo de identidad.



Hacker Épico

Alejandro Ramos / Rodrigo Yepes

Oxword • 20€ • 25 € el cómic

Mezcla de novela negra y manual de alto nivel técnico, esta obra de Alejandro Ramos y Rodrigo Yepes se postula como otro título imprescindible en la biblioteca de cualquier hacker. También disponible en versión cómic – una joya de 168 páginas con ilustraciones del genio Eve Maetrata desde temas relacionados con los sistemas y análisis forense hasta técnicas depuradas de hacking web, todo ello desde la más estricta rigurosidad.



Esteganografía y Estegoanálisis

Jordi Serra y Daniel Lerch

Oxword • 20€

Las técnicas esteganográficas han sido, durante la historia del espionaje internacional, las más eficaces para enviar mensajes ocultos a través de una infinidad de formatos, desde tatuajes hasta cartas. Inventadas en la antigua China, se han usado en conflictos diplomáticos, espionaje empresarial y hasta en ataques terroristas como los del 11-S en Nueva York. Este libro muestra un completo recorrido de la historia de estas técnicas, desde sus inicios hace miles de años.

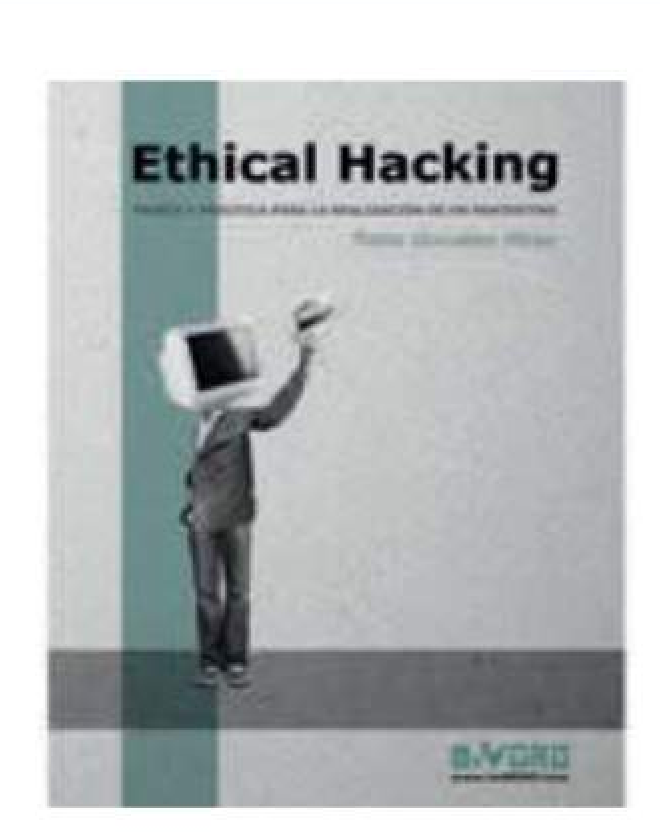


¡Atención mamás y papás!

Ángel Pablo Avilés / Kepa Paul Larrañaga

Ed. Thomsom Reuters • 16,5€

Guía práctica imprescindible para dar respuestas rápidas y concretas a padres y madres, con hijos e hijas usuarios de dispositivos móviles: smartphones, tablets y wearables. Ofrece 60 sobre situaciones de uso posibles de dispositivos móviles por niños, niñas y adolescentes, y analizadas sobre los tres espacios donde habitan éstos: la familia, la calle y la escuela o instituto.



Ethical Hacking. Teoría y práctica para la realización de un pentesting

Pablo González Pérez

OxWord • 20€

La obra propone un enfoque distinto al estudio y aplicación del hacking ético a través de procedimientos, procesos, vectores de ataque, técnicas de hacking, teoría y práctica de esta disciplina. Todo ello permite llevar a cabo acciones maliciosas envueltas en la ética profesional de un hacker que ha sido contratado con el fin de encontrar los agujeros de seguridad de los sistemas de una organización.

EL MUNDO ESTÁ SIENDO ATACADO

Sólo en 2014, se calcula que las empresas europeas perdieron cerca de 14.000 millones de euros por culpa de ciberataques, de los que tardan en recuperarse, de media, casi tres meses. Estas son las amenazas que las grandes compañías de ciberseguridad han detectado en los últimos meses -y que continúan activas-... y sus previsiones cibermeteorológicas para 2016.

// Texto: Santiago Lauja

TREND MICRO

Qué amenazas estarán de moda en 2016. La firma estadounidense ha alertado sobre que las ciberamenazas que más crecerán serán: la extorsión online, el hacktivismo –activismo a través de Internet- y el malware móvil –que crecerá hasta los 20 millones de tipos–. En cuanto a las empresas, la tendencia será apostar por un sistema de defensa ofensivo -en vez de defensivo-, respondiendo a un ataque con otro ataque... o realizando una ataque preventivo. El CTO de Trend Micro, Raimund Genes, ha explicado que "tanto gobiernos como empresas comenzarán a ver los beneficios de contar con un plan estratégico capaz de enfrentarse a cualquier riesgo".

CHEETAH MOBILE SECURITY

Tablets 'malignas'. A través de la tienda 'online' Amazon se han comercializado cerca de 15.000 dispositivos –de 30 marcas diferentes-, con sistema operativo Android, infectadas con el peligroso troyano Cloudsota. Su potencial es tal que puede, incluso, desinstalar, entre otras aplicaciones, el antivirus que el dispositivo lleva incorporado de serie. El país más afectado por este troyano es México, aunque según el Laboratorio Cheetah Mobile Security, estas tabletas se han vendido en 153 países. Si la tuya comienza a mostrar publicidad sin abrir el navegador o mientras navegas, pero de forma anormal... deberás reinstalar el software.

KASPERSKY

El ataque más largo del año. El laboratorio de la firma ha detectado un ciberataque que ha durado 320 horas de forma ininterrumpida. Era de tipo DDoS –ataque distribuido de denegación de servicio-, y su objetivo era 'tumbar' webs de 79 países -los efectos más dañinos los vivieron en China, EE.UU. y Corea del Sur-. El número máximo de ataques contra una misma víctima ha sido de 22: los sufrió un servidor ubicado en los Países Bajos. "Hemos registrado ataques de gran complejidad contra bancos, pero hay nuevos métodos de bajo coste diseñados para interrumpir las operaciones de una empresa por un tiempo concreto", ha explicado Evgeny Vigovsky, jefe de Protección DDoS de Kaspersky , quien también ha recordado que "el número de ataques de gran duración, capaces de quebrar un gran negocio irá en aumento".

T-MOBILE

Ojo a tus datos. Piratas informáticos han sustraído datos de cerca de 15 millones de clientes de la compañía estadounidense T-Mobile, que contrataron sus servicios entre septiembre de 2013 y septiembre de 2015. Los criminales se apoderaron de nombres, fechas de cumpleaños y direcciones de los clientes así como su número de la seguridad social, carnet de conducir y pasaporte.

IBM

Los números. Cada día se descubren 250.000 virus y se monitorizan 15.000 millones de incidencias, según los datos de la presidenta de IBM España, Marta Martínez Alonso, cuya empresa detecta a diario en torno a 1,7 millones de ataques en todo el mundo. "Además del impacto económico, lo relevante es que, desde un punto de vista tecnológico, los cibercriminales tienen como objetivo la información", destaca.

SYMANTEC

Los sectores en peligro. Según el informe Intelligence Report, que analiza las amenazas de los últimos meses de 2015, las organizaciones financieras e inmobiliarias son el principal objetivo de los ciberataques -27%-. En cuanto al phishing -el robo de información haciéndose pasar por otra persona o entidad en un correo electrónico-, el objetivo han sido las grandes empresas -45,7%, frente al 11,7% de meses anteriores-. Los sectores más atacados son los de Agricultura, Silvicultura y Pesca, tanto por medio de campañas de phishing como de malware. De hecho, uno de cada 988 correos electrónicos fue un intento de phishing, y uno de cada 308, contenía malware -software malicioso-. El sector de la minería, que incluye la extracción de petróleo y gas, tuvo la tasa más alta de spam -correo basura, no deseado-, con el 55,8%.

CCN-CERT

Cuidado con tu móvil. En su 'Informe de Amenazas a telefonía móvil' de 2015, el organismo del CNI ha alertado sobre la vulnerabilidad Stagefright, "la más crítica en la historia de Android", que afecta al 95% de móviles y tablets. Se trata de un fallo de seguridad que permitiría hackear estos dispositivos. ¿La forma de evitarlo? Configurar bien el teléfono, realizar copias de seguridad y tener la última versión de su sistema operativo.

LOOKOUT

Aplicaciones falsas. La firma ha identificado tres tipos de malware para móviles Android, en 20.000 aplicaciones de Google Play que ha analizado. Su forma de actuar es instalarse en el dispositivo y hacerse pasar por apps como Facebook, Candy Crush, Twitter, Snapchat y WhatsApp y mostrar todo tipo de publicidad.



LOS 10 ATAQUES EN ESPAÑA QUE MÁS DEBEN PREOCUPARTE

"España sufre un tipo de ataque similar al resto de las naciones occidentales. Eso sí, hay que destacar que en los últimos meses los ataques de tipo ransomware -los que cifran la información del ordenador y piden un rescate por ella- han crecido hasta la quinta posición de riesgos", explica el director general de Check Point, Mario García. Esta empresa ha elaborado su top 10 de los ataques de malware que han afectado a particulares, empresas y organismos en los últimos meses de 2015.

1 **CONFICKER.** Es un gusano, descubierto a finales de 2008, que dirige sus ataques a plataformas Windows. Las variantes de este tipo de virus permiten la descarga de malware y que los ciberdelincuentes tomen el control de la máquina infectada.

2 **KELIHOS.** Se trata de una botnet -una red de robots informáticos que se ejecutan de forma automática- que atenta generalmente contra plataformas Windows. Es anterior a 2010 y, aunque ha sido desactivada en varias ocasiones, siempre ha vuelto a aparecer. Utiliza comunicaciones P2P -que permiten el intercambio directo de información entre ordenadores- para ataques de denegación de servicio, spam y robo de monederos de Bitcoin, entre otros.

3 **ZEROACCESS.** Descubiertos en 2012, son gusanos que dirigen sus ataques a plataformas Windows con la ejecución de código remoto y la descarga de malware, a través del servidor de Comando y Control -C&C- o bien vía P2P. Se ejecuta en niveles bajos del sistema operativo, por lo que es resistente a los sistemas habituales de seguridad.

4 **TEPFER.** Es un troyano para Windows que abre una 'puerta trasera' para rastrear y robar información privada o para controlar remotamente el ordenador. Descubierto en 2012, se dirige principalmente a plataformas Windows y suele introducirse en el sistema a través de spam o phishing.

5 **CRYPTOWALL3.** Un ransomware descubierto este mismo año, generalmente distribuido a través de ataques drive-by -en descargas-. Primero cifra los archivos de la máquina infectada y luego informa al usuario que tiene que pagar un rescate para recibir una clave de descifrado.

6 **SINOWAL.** Un troyano resistente, cuyas primera referencias son anteriores a 2009. En sus inicios, llegaba en un email sobre la gripe porcina, solicitando al usuario crear un perfil personal accediendo a cierta página web. Otras variables están diseñadas para robar información confidencial.

7 **ZEMOT.** Descubierto en 2014, es un 'descargador' de troyanos que forma parte de una red compleja, que incluye diferentes tipos de malware. Una vez penetra en los sistemas, su objetivo es realizar fraude -generando clics en determinadas webs-. Algunas de sus variantes han sido utilizadas para descargar nuevo malware y robar información sensible.

8 **ASPROX.** Una botnet activa desde el año 2007, que se enfoca principalmente en el phishing y el fraude electrónico. Permite realizar ataques de phishing, ataques de inyección SQL -sobre bases de datos- para distribuirse a sí misma y descargas de software "pay-per-install" para generar ingresos.

9 **CUTWAIL.** Es una familia de troyanos dirigidos a plataformas Windows, descubiertos en 2007. Su operativa primaria son ataques DDoS y spam, pero variantes posteriores pueden ejecutar códigos remotamente y recopilar información sensible. Emplea un rootkit para evitar su detección y eliminación.

10 **SALITY.** Descubierto en 2003, es uno de los troyanos más longevos. Sus variantes permiten la ejecución remota de código y la descarga de malware. Su principal objetivo es persistir en el sistema infectado y facilitar su control remoto a través de su servidor de comando y control.

TE SERÁ ÚTIL

SYMANTEC, AMENAZAS EN TIEMPO REAL

La firma de ciberseguridad tiene varios centros de control que supervisan y analizan qué está pasando en el ciberespacio en tiempo real. En total, monitoriza ocho billones de objetos, de los que extrae posibles ciberamenazas, identifica malware y supervisa y protege los dispositivos con los que trabaja. Por ejemplo, su antivirus Norton -uno de los más vendidos- cuenta con unos 110 millones de clientes, entre particulares y empresas. Y es que, como explica el CEO y presidente de Symantec, Michael Brown, "cuanto más sabes de amenazas mejor puedes proteger a tus clientes".

FIREFOX TE AYUDA A EVITAR QUE TE ESPÍEN

El conocido navegador ha comenzado a ofrecer una nueva funcionalidad que bloquea anuncios, rastreadores y botones sociales que pueden registrar información particular del usuario, para evitar el rastreo por parte de terceros. La nueva opción -disponible para sistemas operativos Windows, Mac, Android y Linux- está dentro de la llamada 'aplicación privada', incorporando una capa más de protección.

GMAIL TE ALERTA DE LOS CORREOS SIN CIFRAR

Gmail ha prometido una nueva medida de seguridad que consiste en avisar si llega uno de esos correos sin cifrar –en los que puede ir software malicioso-. De esta forma, el usuario será consciente de que dicho correo será de fácil acceso a cualquiera que intercepte la comunicación. Eso sí, el servicio te avisará... pero no te impedirá abrirlo, ni evitará que te infecten el ordenador o el teléfono.

8 DATOS SOBRE CIBERSEGURIDAD EN ESPAÑA QUE NO CONOCÍAS

Nuestro país encabeza todas las listas relacionadas con cibercrimen y sus consecuencias. La empresa Buguroo te muestra en esta infografía datos sobre la ciberseguridad en nuestro país que probablemente desconocías.



1 ¿LA SEGURIDAD? ¿IMPORTANTE? ¡QUÉ VA!

El 33% de los usuarios no presta atención al nivel de seguridad de los sitios web ni dispone de un software antivirus en su smartphone o tablet.



2 LA INDUSTRIA Y LA CIBERSEGURIDAD NO HACEN BUENAS MIGAS

Sólo el 17% de las empresas industriales en España cuenta con un plan de gestión frente a ciberataques. Un 5,6% de ellas afirma no saber si lo tiene.



3 MEDALLA DE BRONCE EN MALWARE BANCARIO

España es el tercer país europeo con mayor porcentaje de ataques. Concretamente, el 22% de los ataques en Europa tiene lugar en nuestro país.

INFOGRAFÍA:



LOS CIBER CRIMINALES BUSCADOS POR EL FBI

Carlos Enrique Pérez-Melara Joven salvadoreño buscado por, supuestamente, crear una web que permitía a sus clientes descubrir si su pareja le era infiel enviando una tarjeta electrónica a la víctima. Una vez abierta la tarjeta, se instalaba un programa espía, denominado primero "Email PI" y luego "Lover Spy", de forma oculta, el cual enviaba información de contraseñas, emails enviados y páginas web visitadas a la persona que había contratado el servicio. El FBI acusa a Pérez-Melara de interceptar ilegalmente las comunicaciones electrónicas, de acceder sin autorización a ordenadores protegidos con el objetivo de lucrarse y de fabricar y enviar un dispositivo oculto, entre otras cosas. **El FBI ofrece 47.000 euros a cambio de información sobre él .**





4 PROBABLEMENTE TU BANCO HA SUFRIDO UN CIBERATAQUE

8 de los 10 principales bancos y cajas de ahorros del país han reconocido ciberataques en el último año. El 60% del fraude con tarjetas bancarias proviene de compras por internet.



5 LA COMIDA SIEMPRE ES LA CLAVE

Somos los terceros en elegir más frecuentemente como contraseña nuestra comida favorita. Con tan solo 10 intentos, un hacker podría tener un 19,7% de probabilidades de acierto al descifrarla.



6 CASI LA MITAD DE NUESTRO SOFTWARE ES ILEGAL

La nada despreciable cifra del 45% del software instalado en España es ilegal y un alto porcentaje del malware se distribuye a través del mismo.



7 RECIBIMOS CERCA DE 20K ATAQUES AL AÑO...

En 2014, el Ministerio del Interior detectó 18.000 ciberataques, de los cuales 63 eran de especial gravedad y 4 afectaban a la industria nuclear.



8 ...PERO TAMBIÉN SE NOS DA BIEN GENERARLOS

España es el séptimo país de Europa y el decimoquinto del mundo que más ciberataques genera. La forma más extendida es el spam, seguida de bots y phishing. La extorsión mediante ransomware ha crecido un 113%.

Evgeniy Mikhailovich Bogachev, Está acusado de extorsión, robo de identidad, fraude electrónico y bancario, lavado de dinero... Bogachev, supuestamente, instalaba sin autorización el virus 'Zeus' en los ordenadores de sus víctimas. Con él, se hacía con contraseñas, número de identificación personal y números de cuentas bancarias para registrarse en las webs de distintas entidades bancarias. **El FBI ofrece por información sobre él 2,8 millones de euros.**

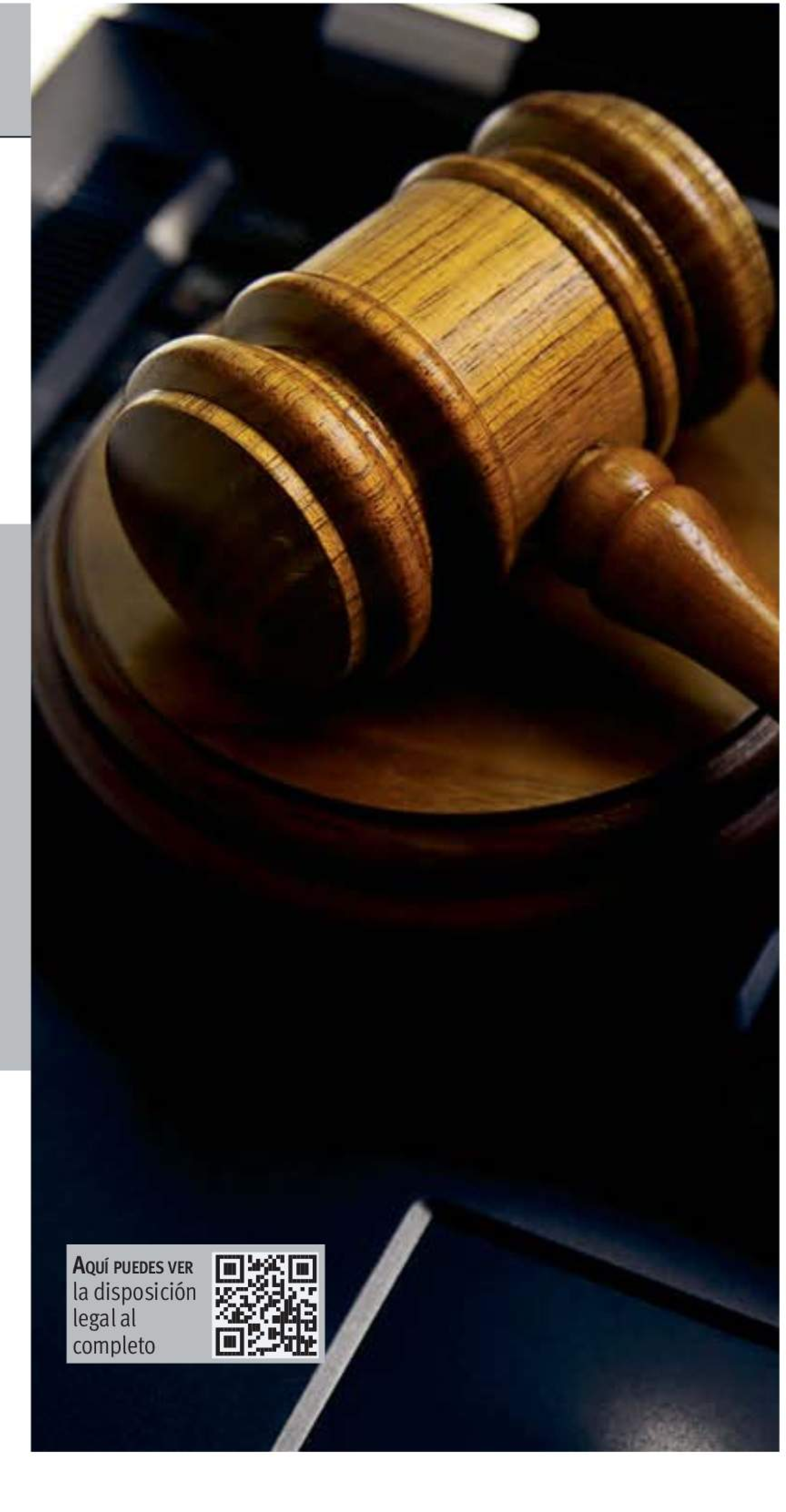
Bjorn Daniel Sundin y **Shaileshkumar P. Jain** Se encuentran entre los más buscados por estar supuestamente involucrados en una operación en la que defraudaron a usuarios de Internet de más de 60 países. Colocaban falsos anuncios en páginas web verdaderas y hacían creer a sus víctimas que sus ordenadores estaban infectados con malware, para hacerles comprar sus productos, provocando pérdidas de más de 94 millones de euros. **El FBI ofrece por información sobre cada uno casi 20.000 euros.**

Alexsey Belan Fue acusado de hackear las redes de tres grandes tiendas online en Estados Unidos. Según el FBI, también robó sus bases de datos en la que había contraseñas y datos personales de millones de personas, para venderlos. **Se ofrece por información sobre él 90.000 euros.**

Nicolae Popescu Ciudadano rumano buscado por, presuntamente, haber participado en un fraude a través de Internet. Popescu robaba millones de dólares a través de una supuesta web de subastas en la que ofrecía productos de gran valor como coches o barcos que en realidad no existían. **El FBI ofrece casi un millón de euros a cambio de información que lleve a su captura.**

ASÍ TE AYUDARÁ A DEFENDER TU VIDA PRIVADA EN INTERNET

YA SE APLICA EL PRIMER 'CIBERCÓDIGO' PENAL



Desde julio de 2015, entrar en un ordenador que no sea tuyo puede ser igual de grave que hacerlo en una vivienda ajena. El nuevo texto legal endurece las penas por delitos informáticos. Si quieres saber cómo te afecta, qué nuevos derechos tienes y qué delitos podrías cometer en el mundo virtual sin darte cuenta, toma nota. Recuerda que, además, en diciembre entra en vigor la nueva Ley de Enjuiciamiento criminal.// **Texto: D. Noriega**

La evolución tecnológica te facilita la vida, pero también te deja más expuesto ante los ciberdelincuentes que quieren apropiarse de tu vida privada en el ciberespacio, a través de las fotos y comentarios que haces en redes sociales, consultas en buscadores que quedan registradas, contraseñas, etc. Para protegerte de estos criminales, que trabajan en un mundo hasta ahora sin legislar, el nuevo Código Penal, en vigor desde el 1 de julio de 2015, aborda los delitos informáticos que ya se producen y se adelanta a otros... para atajarlos antes de que se cometan y de que no tengan solución. Precisamente, la importancia histórica de este nuevo texto es que permitirá "dar respuesta a delitos que se pueden producir 'en la nube' o a través de las nuevas tecnologías. Con él, el Derecho Penal ha dejado de ser exclusivamente represivo: además de castigar al culpable tras cometer el delito... se actuará de forma preventiva", explica el magistrado de la Audiencia Nacional, Eloy Velasco. En una jornada sobre las modificaciones del Código organizada por la Asociación Profesional Española de Privacidad -APEP-, el magistrado Velasco y la fiscal Tejada desvelaron la letra pequeña, para que sepas qué hacer en cada caso.

AHORA, LAS MULTAS A LAS EMPRESAS QUE COMETAN DELITOS SON MÁS ELEVADAS

Según el abogado Marcos Mª Judel, vicepresidente 2º de la APEP las multas ascienden a:

De tres a cinco años a quien descubra secretos o vulnere la intimidad de las personas acce-



'TROYANOS POLICIALES'

La nueva Ley de Enjuiciamiento criminal permitirá usar este software, siempre con autorización judicial, por parte de los cuerpos y fuerzas de seguridad. Se utilizará para recabar pruebas en los teléfonos y equipos informáticos de presuntos delincuentes. Ello permitiría, por ejemplo, activar la webcam del PC o el móvil de un delincuente para grabar hechos delictivos en los que podría estar presente; un sistema que "ya se usa en países como Colombia", explica el fiscal Jorge Bermúdez.

diendo a su correo electrónico, mensajes o interceptando sus comunicaciones.

Hasta dos años a quien, sin permiso, vulnere medidas de seguridad o de acceso a un sistema de información [...] o diseñe o adquiera programas para lograrlo.

Hasta tres años al que interrumpa u obstaculice, sin autorización, el funcionamiento de un sistema informático.

Hasta cinco años al que, sin permiso, borre, dañe, altere o bloquee programas o documentos informáticos causando graves daños o afectando a muchos sistemas.

Sin embargo, si es una persona la que resulta condenada, el máximo es dos años de multa.

1 MÁS DUREZA CONTRA LOS CRIMINALES. Por primera vez se diferencia de forma clara lo que es un delito de robo de documentos e información... de un ciberataque contra una infraestructura crítica -la red ferroviaria, una central eléctrica, el sistema de control del tráfico, etc-. ¿La pena? Hasta ocho años de prisión para los casos en los que se ponga en riesgo la Seguridad Nacional.

2 CIBERJUECES. Se les da la facultad de acordar, de forma inmediata, el bloqueo del acceso a una web o la retirada de un contenido si consideran que hay indicios de delito. Una situación que se producirá entre otros casos, en los que haya un posible delito de odio contra colectivos -judíos, personas de otras razas, mujeres, etc.- y que, hasta ahora, no se retiraba hasta el día de la sentencia.

3 OJO A LO QUE ENVÍAS A TUS AMIGOS... ya que se considera delito difundir imágenes o vídeos íntimos sin el consentimiento de su protagonista, aunque, en su momento, sí hubiera aceptado la grabación. Así, publicar en redes sociales o por W hatsApp cualquier imagen íntima de una expareja que hayas grabado estando con ella será perseguido.

4 TU INTIMIDAD VA MÁS ALLÁ DE LO SEXUAL. Se considera como tal cualquier dato o información que pueda afectar a la vida privada. Por ejemplo, el robo de las contraseñas de las redes sociales; también, si 'subes' o reenvías imágenes de una borrachera con los amigos sin el permiso de todos los que aparezcan.

5 PORNOGRAFÍA INFANTIL Y VIRTUAL. Se considera 'pornografía infantil' cualquier imagen de menores en conductas reales, explícitas o simuladas de carácter sexual, incluyendo a quienes, no siendo menores, están afectados por algún tipo de discapacidad.También se consi-

dera 'pornografía técnica o virtual' la que representa a menores. Y no sólo eso: se perseguirá tanto al que se descarga contenidos pedófilos como al que tan sólo los ve en Internet sin bajárselos a su dispositivo.

6 PROBLEMAS CON LOS PROGRAMAS DE TU ORDENADOR. Se considerará delito y se actuará contra quien guarde en sus dispositivos programas maliciosos que faciliten ataques informáticos masivos. Eso sí, la 'letra pequeña' dice que "debe tener que demostrarse que se tiene con el fin de cometer un delito", destaca Tejada. Así, podrías ser condenado por guardar, por ejemplo, software que permita clonar tarjetas, robar contraseñas informáticas o tener aparatos que se venden en tiendas o por Internet para interferir señales wifi. Son "programas cuya justificación legal es complicada de defender, ya que están diseñados para estafar", explica Velasco, recordando que en estos casos se actuará antes de que se cometa el delito con ellos.

7 NUEVOS DELITOS CONTRA LA PROPIEDAD INTELECTUAL. Se protege no sólo a los autores o inventores de un producto o servicio, sino también a los intermediarios.

8 ALLANAMIENTO DE DISPOSITIVOS. Acceder a tus aparatos electrónicos -móviles, tablets, ordenadores, etc.- sin tu permiso, será un delito que pasará a ser igual "que entrar en tu casa sin tu permiso, aunque no sea para delinquir", destaca Velasco.

9 CUIDADO CON LO QUE DICES. Se considera que puede ser delito la difusión de mensajes o consignas que inciten a la alteración del orden público. Una situación que se agrava si se trata de consignas con fines terroristas; sobre todo, si pueden afectar a la seguridad de infraestructuras críticas.

10 ATENTO A LO QUE HACEN LOS TRABAJADORES. Se pedirán responsabilidades a las empresas de los comportamientos delictivos que hagan sus empleados en su trabajo o con sus medios. Por ejemplo, si desde el ordenador de la oficina realizan espionaje industrial, algún tipo de estafa informática, difusión de secretos... En estos casos se actuará contra la persona... y contra su compañía.

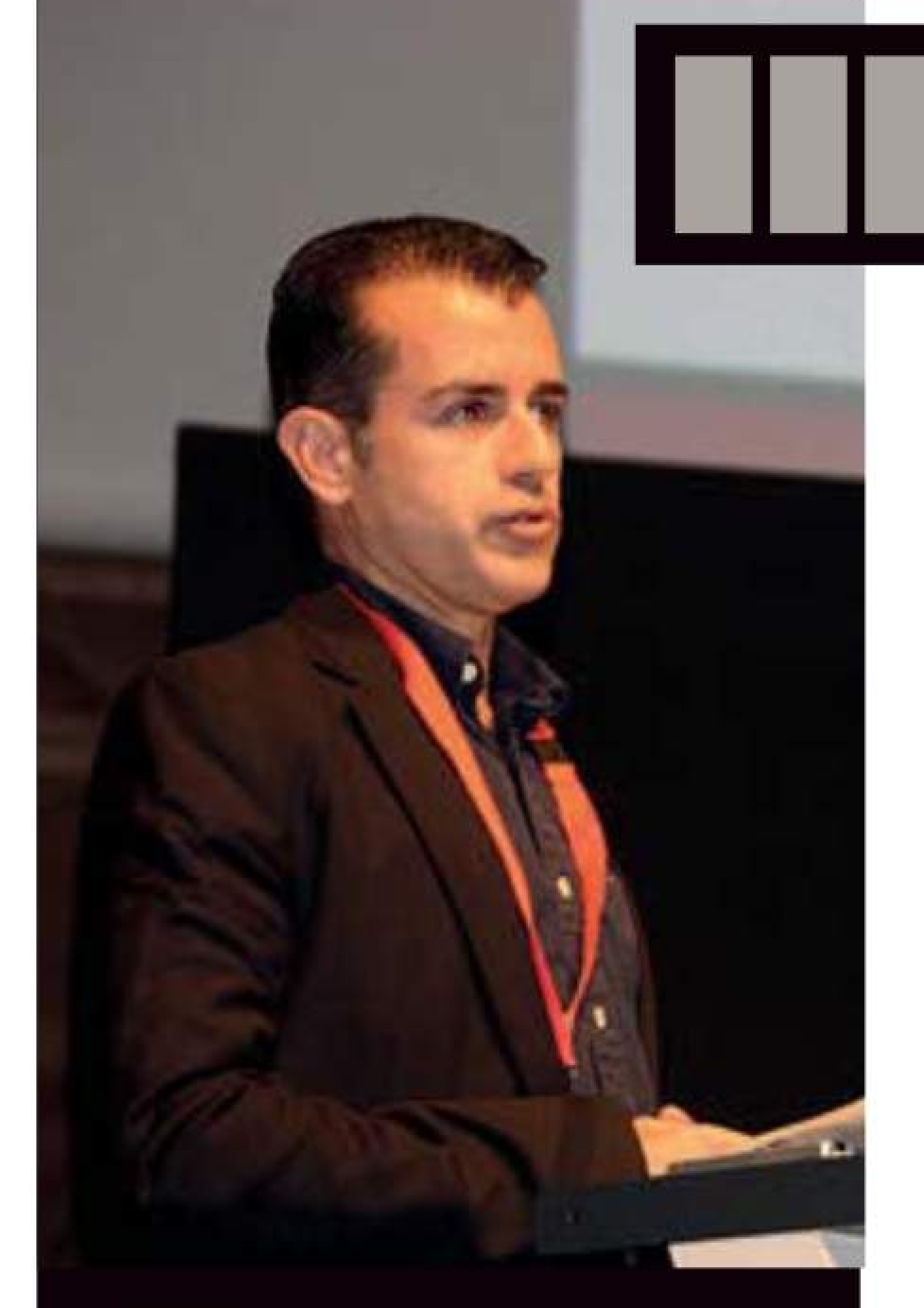
GRABAR CONVERSACIONES SIN COLOCAR MICRÓFONOS

Con la nueva Ley de Enjuiciamiento Criminal podrán 'activarse a distancia' los micrófonos de los teléfonos móviles a los que se haya accedido por programas informáticos, siempre con autorización judicial. Ello permitirá grabar las conversaciones de los delincuentes a los que se persiga. "Ya no tiene sentido que un agente se juegue la vida entrando en una casa para colocar un micrófono. Incluso, puede activarse el micrófono del móvil, según el lugar en el que esté, a través del GPS que incluyen los actuales teléfonos inteligentes", explicó en Rooted.CON el fiscal del Servicio de criminalidad Informática, Jorge Bermúdez.


FOTO: U.S. MARINE CORPS PHOTO BY SGT GUADALUPE M. DEANDA III

INTERCEPTAR LLAMADAS POR SKYPE Y OTRAS REDES

Los jueces también podrán autorizar que la policía intercepte redes de comunicaciones virtuales. ¿Qué significa? Pues que se podrán intervenir, por ejemplo, llamadas por Skype. Curiosamente, también se establece la obligación de cualquier experto informático de colaborar con los agentes para poder conocer con exactitud los medios empleados por los criminales. "¿Estamos hablando ya de hacking judicial? De ser así, siempre se hará de forma amable. Aunque tal vez en este tema no se pueda 'doblar el brazo' a una persona para que colabore" con la Justicia, destaca Bermúdez.



CARLES SOLÉ,

DIRECTOR CENTRO DE ESTUDIOS CIBERSEGURIDAD ISMS FORUM

CHAQUETA V

AÑOS 41, a mi pesar.
ESTUDIOS: Ingeniería Superior Informática y MBA.
EMPRESA Y CARGO: CaixaBank – Director de Seguridad de la Información.
TE GUSTA VESTIR CON... Ropa casual y, a poder ser, sin corbata.
RELOJ Un viejo chrono al que pronto tocará jubilar.
PC, APPLE/ANDROID O IOS -Y POR QUÉ- En casa, Apple. Lo sacas de la caja, lo enciendes y funciona durante años.
UN TRUCO PARA EVITAR CIBERATAQUES Nada que no hagamos en el mundo real: sospechar de lo desconocido.
EL EXPERTO AL QUE MÁS ADMIRAS... Al que, además de bueno, es capaz de transmitir su mensaje.
TU SECRETO PARA SER EL MEJOR... ¡Ojalá lo conociera! Por suerte, trabajo con los mejores.
TE APASIONA... Aprender cosas nuevas. Y cuánto más diferentes entre ellas, mejor.

1 ¿QUÉ ES PARA TI UN HACKER? ¿TE CONSIDERAS UNO DE ELLOS?

Me gusta pensar que, como mínimo, tengo en común la pasión por entender cómo funcionan las cosas, algo inherente a la idiosincrasia de un hacker. Pero para nada tengo la experiencia, la dedicación ni los conocimientos de alguien que pueda considerarse un verdadero hacker. Para mí, estos profesionales son auténticos expertos en aplicaciones, sistemas y redes capaces de utilizar y combinar sus habilidades para llegar hasta lo más profundo de cómo se comporta una determinada tecnología. El error, demasiado común, es asociar el concepto de hacker a quienes cometen delitos. Esto ya dependerá de para qué se utilice el conocimiento obtenido, como pasa con todo conocimiento humano.

2 ¿QUÉ ES LO QUE MÁS TE PREOCUPA EN EL MUNDO DE LA CIBERSEGURIDAD?

Creo que estamos ante dos grandes problemas de raíz: El primero, la falta de mecanismos fiables -y usables- para conocer la identidad real de la persona que interactúa con nosotros o con/contra nuestras estructuras a través de Internet. El segundo, la complejidad de las aplicaciones y los sistemas, que hace que esa esperanza que teníamos hace algunos años sobre software libre de vulnerabilidades se haya desvanecido. Y si lo primero proporciona anonimato a los cibercriminales, lo segundo les ofrece un sinfín de posibilidades para perpetrar sus cibercrímenes. Aunque la esperanza es lo último que se pierde y es posible que, con los años, lleguemos a un modelo suficientemente maduro donde los riesgos sean equiparables a los del mundo real.

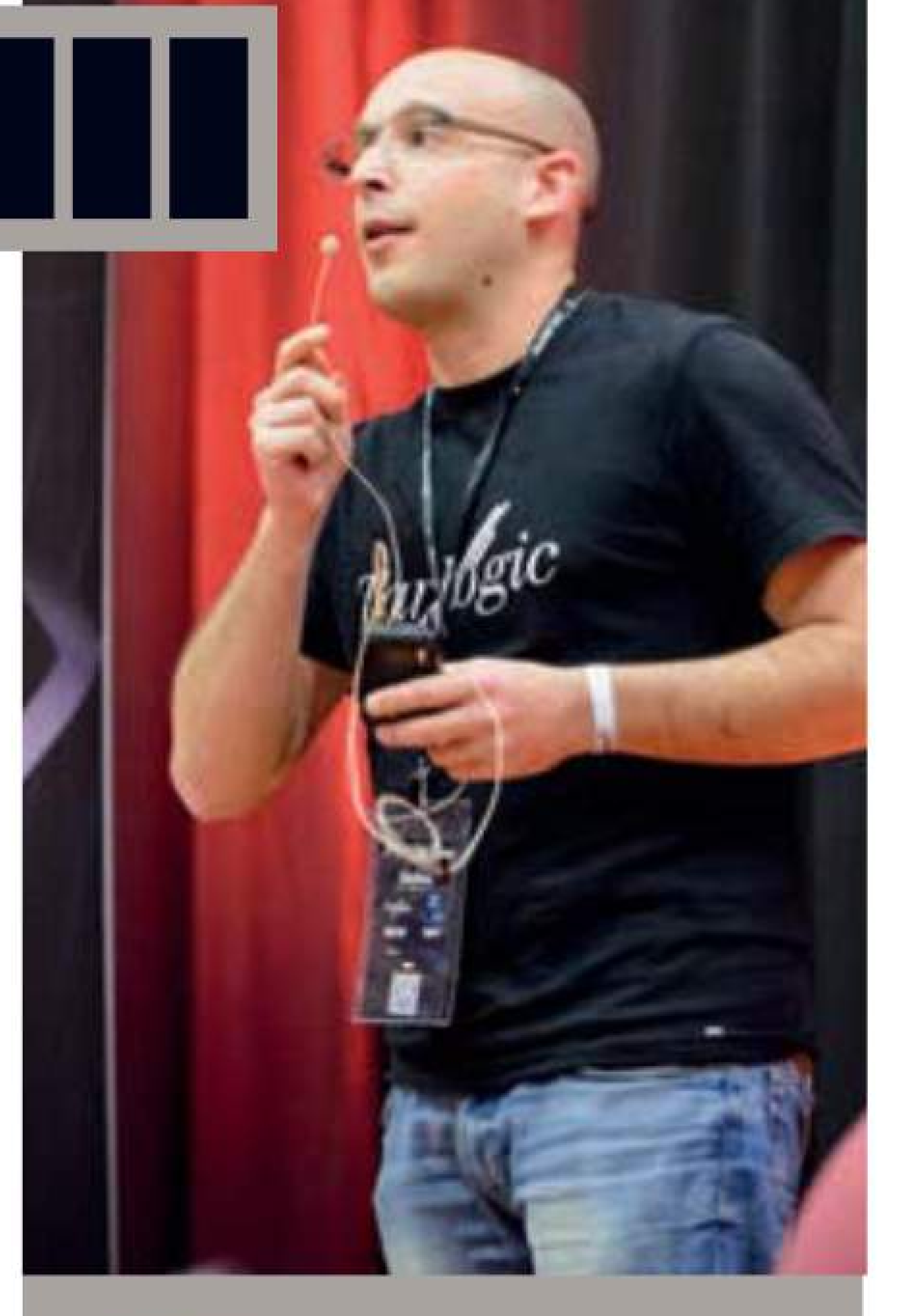
3 ¿QUIÉN TIENE QUE MANDAR MÁS EN UNA EMPRESA: EL JEFE DE SEGURIDAD FÍSICA O EL DE SEGURIDAD INFORMÁTICA?

¿Necesariamente? Ninguno de los dos. Ambos tienen que liderar equipos, internos o externos, y tomar decisiones, a poder ser certeras y, la mayoría de las veces, en el menor tiempo posible. Cada uno en sus respectivos ámbitos y bajo parámetros que pueden ser muy diferentes, pero persiguiendo un objetivo común: la protección de los clientes, los empleados y la propia empresa. Lo que sí resulta cada vez más necesario es el entendimiento mútuo y el disponer de los canales adecuados para coordinarse de forma ágil y efectiva entre ellos. Especialmente en la respuesta ante incidentes y en la visión global del estado de la seguridad. Y si de algo no me cabe la menor duda, es de que podemos aprender mucho los unos de los otros.

4 QUÉ LE PIDES SOBRE CIBERSEGURIDAD AL PRÓXIMO GOBIERNO.

Que actúe contra los cibercriminales. Son grupos muy bien organizados, pero dejan trazas y pistas suficientes cómo para conocer cómo y desde dónde nos atacan. Sin embargo, los recursos para perseguirlos y las barreras a una coordinación internacional efectiva, nos dejan indefensos a ciudadanos y empresas. Durante muchos años se ha hablado de compartir información -reputación, IOCs, muestras de malware-, pero se ha avanzado muy tímidamente al no existir, a mi parecer, plataformas neutrales y con suficientes garantías para poder hacerlo. Tenemos que dejar de hablar y pasar a la acción efectiva.





ANDRÉS TARASCO, SOCIO FUNDADOR DE TARLOGIC

S CAMISETA

1 ¿TE CONSIDERAS UN HACKER?¿QUÉ ES PARA TI UN HACKER?

Los hackers son personas inquietas, con habilidades para analizar problemas de forma poco convencional y con una necesidad de conocer cómo funciona cualquier sistema y de compartir el conocimiento.

En el campo técnico, un hacker estudia y aprovecha el funcionamiento de sistemas de forma poco convencional para alterar su funcionamiento normal. Este conocimiento y esta habilidad es el utilizado para proteger sistemas informáticos de las empresas y de los usuarios y del robo de información. Como en todos los campos, siempre hay gente que usa sus conocimientos con fines ilícitos, pero son una minoría y va en contra del espíritu hacker.

Soy un apasionado del hacking y siempre quiero saber sobre cómo funciona la tecnología, aunque la realidad del trabajo en el día a día me están conviertiendo más en un gestor de equipos.

2 ¿QUÉ ES LO QUE MÁS TE PREOCUPA EN EL MUNDO DE LA CIBERSEGURIDAD?

La posibilidad de perder el control de nuestros datos y comunicaciones. Protegerse de ataques y espionaje gubernamental es una tarea compleja, pero la fuga de cerebros que estamos viendo en nuestro país debido a la crisis dificulta mucho poder ofrecer servicios especializados a las empresas y cubrir una demanda real.

Dado que cada vez los sistemas informáticos toman mas relevancia en el funcionamiento de cualquier empresa, perder el conocimiento y los especialistas en ciberseguridad puede provocar que seamos menos competitivos en el futuro y que seamos más vulnerables al espionaje industrial.

3 ¿QUIÉN TIENE QUE MANDAR MÁS EN UNA EMPRESA, EL JEFE DE SEGURIDAD FÍSICA O EL DE SEGURIDAD INFORMÁTICA?

No creo que el responsable de seguridad física tenga capacidad para analizar las tecnologías o las implicaciones de ciertas decisiones desde el punto de vista de seguridad informática. Ambas áreas tienen su importancia estratégica y deben trabajar conjuntamente.

4 QUÉ LE PIDES SOBRE CIBERSEGURIDAD AL PRÓXIMO GOBIERNO

Que apueste por la formación de profesionales en ciberseguridad y que colabore con el sector privado para proteger a los ciudadanos y a nuestras empresas del espionaje y robo de información. Aunque a corto plazo las decisiones que tome no generen un marco de incertidumbre en el sector, ya que se barajan cambios normativos relacionados con la ley de seguridad privada que supeditarían la ciberseguridad a la seguridad física y harían desaparecer a todas las pymes e investigadores en involucradas en el campo de la ciberseguridad.

AÑOS 36.
ESTUDIOS: He sido autodidacta. No he finalizado los estudios de Ingeniería informática, ya que el último año abandoné la carrera por la oportunidad de formar parte de un gran equipo de gente especialidado en seguridad informática.También he cursado el master de Director de seguridad por la UNED.
EMPRESA Y CARGO: Desde hace cuatro años soy socio fundador de Tarlogic Security, y dirijo el área de ciberseguridad
TE GUSTA VESTIR CON... Vaqueros y camiseta
RELOJ No uso desde que tengo teléfono móvil, aunque siempre me han gustado los relojes analógicos.
PC, APPLE/ANDROID O IOS -y por qué- Android, porque puedes instalar cualquier software sin dejar expuesto tu teléfono por haberte saltado las restricciones con las que viene tu sistema operativo.
UN TRUCO PARA EVITAR CIBERATAQUES Actualizar todo nuestro software, y tener sentido común. Debes borrar cualquier documento sospechoso o programa que no sea de confianza.
EL EXPERTO QUE MÁS ADMIRAS: En España, le tengo un aprecio especial a la gente del equipo Intr3pids y de 48bits. Fuera de España, Kevin Mitnick y Elias Levy han sido una inspiración para mi.

10 CONSEJOS PARA QUE TUS VACACIONES NO SEAN UN INFIERNO

EVITA QUE TE ROBEN DINERO EN TUS COMPRAS

En Navidades es cuando los cibercriminales trabajan más duro. Es la época del año en la que más operaciones se realizan por Internet: desde adquisición de billetes de avión o tren hasta todo tipo de compras. Una puerta abierta para que estos delincuentes 'hagan su agosto' en pleno invierno robando dinero, usurpando cuentas en Facebook y Twitter, secuestrando ordenadores y convirtiendo, a veces, estos días de felicidad... en un infierno para sus víctimas. ¿Cómo lo hacen... y cómo puedes defenderte? // Texto: Elisa Coello



Planear unas vacaciones en estos días es más fácil que nunca. Los usuarios ya no dependen de las recomendaciones de familiares o de lo que le aconsejen desde la agencias de viajes: ahora, basta con un ordenador, una conexión a Internet y unos minutos de tiempo para planificar unos días de ensueño. Sin embargo, esta mayor facilidad también conlleva un mayor riesgo; según los expertos de Kaspersky Lab -empresa especializada en antivirus y software de seguridad-, son muchos los estafadores que buscan víctimas inocentes entre todos aquellos que o compran sus regalos por Internet o contratan los viajes.

LOS CRIMINALES SE APROVECHAN DE LA CODICIA HUMANA PARA ENGAÑAR A LOS USUARIOS CON FALSAS OFERTAS


Consulta las
últimas estafas
por Internet.

APRENDE A DEFENDERTE DEL SPYWARE

Todas las recomendaciones son comunes para este tipo de amenazas externas: un buen antivirus -como los de Eset, Symantec, Kaspersky, Panda, etc.- , un cortafuegos eficaz, navegar por páginas web seguras, no abrir correos de remitentes sospechosos o desconocidos y no instalar nunca programas desconocidos. Y si sospechas que tu ordenador ha sido infectado y que estás siendo espiado, recuerda que los programas espía funcionan mientras estés conectado a la red: desconecta de inmediato la wifi, contacta con tu servicio técnico... ¡y denúncialo! Pero, ¿cómo saber si te espían desde tu ordenador? Si detectas que la luz de tu webcam se enciende sin que tú la hayas activado o si el puntero de tu ratón se mueve de manera errática, la velocidad de navegación es más lenta de lo normal o aparecen iconos desconocidos en tu escritorio... entonces, es posible que tengas un serio problema.

LOS CRIMINALES SE APROVECHAN DE LA CODICIA HUMANA PARA ENGAÑAR A LOS USUARIOS CON FALSAS OFERTAS

1 APRENDE A RECONOCER UNA ESTAFA SI LA TIENES DELANTE

Existen dos formas muy utilizadas por los ciberestafadores para hacerse con el dinero de los usuarios. La primera, y más común, es publicar anuncios en páginas web con productos –casas y coches en venta o alquiler, productos muy demandados como videoconsolas, tabletas, móviles, juguetes…- que, en realidad, no existen. Saber identificarlos es sencillo: verás que tienen un precio que resulta sospechosamente bajo y, cuando se contacta con los supuestos vendedores, éstos exigen una cantidad por adelantado para reservártelo hasta que os veáis. Por supuesto, si abonas ese dinero, nunca volverás a saber de ellos. En el caso de los automóviles, la gente puede llegar a perder entre 3.000 y 5.000 euros en concepto de 'reserva'. La segunda más vista es el 'timo del alquiler': consiste en anunciar pisos y casas para pasar estas fiestas… que ya han sido reservadas en otras webs. Un problema importante, porque la víctima no sabe que ha sido estafada hasta que llega a la casa y se da cuenta de que ya está ocupada.

***CÓMO EVITARLO** Jamás adelantes dinero por Internet sin hablar antes por teléfono con el vendedor y sin tener la seguridad de que es de fiar. Y, por supuesto, huye de los 'super-descuentos'… Casi todos son un gancho para estafar.*

2 PARA PAGAR POR INTERNET, MEJOR CON TARJETA QUE 'ENVIANDO' DINERO….

Muchos estafadores piden que les adelantes el pago de un servicio u objeto enviándoles dinero a través de empresas especializadas en transacciones económicas –MoneyGram, Western Union-. Nunca lo hagas: lo más seguro es que estés mandando el dinero a una dirección real… que no es la del delincuente, pero que éste usará para ir a por el dinero -haciéndose pasar por un vecino, por ejemplo-.

Si lo haces con tarjeta, jamás pagues una transacción si no te piden, además del número de la tarjeta, el código de verificación CVV o CV2 –un número de tres cifras que aparece en el reverso-. ¿Lo ideal? Que, además, te envíen desde tu banco a tu móvil una clave numérica que tendrás que introducir en el momento de realizar la compra y que sirve para certificar la operación. Es lo que se llama 'autentificación de dos pasos'.


***CÓMO PUEDES EVITARLO** Nunca pagues con dinero en efectivo transferencias bancarias o giros postales por servicios o productos de Internet. Utiliza sólo tarjetas de crédito, ya que te concederá un plazo de alrededor de una semana para anular la operación si detectas que te han estafado. Por otro lado, para evitar que alguien 'robe' tu número de tarjeta y clave, y compre con ella en tu nombre, puedes pedir a tu banco las llamadas 'tarjetas monedero' -cuestan unos cinco euros al año-. Se trata de un tipo de tarjeta que se puede recargar con el dinero que necesites en un momento puntual, de forma que si alguien consigue su número, nunca podrá gastar más del saldo que esté disponible en esa tarjeta.*

Por lo demás, apuesta por las webs de comercio electrónico con el sistema de 'pago seguro'. Las reconocerás porque su dirección -en la parte superior del navegador- comienza por "https". Esa 's' final garantiza que la web cumple con los requisitos que garantizan la máxima seguridad de pago.

3 EVITA OFERTAS TENTADORAS Y LAS LLAMADAS 'POP-UPS'

Tu ordenador tiene una conexión segura, un buen antivirus, un cortafuegos –el software que impide comunicaciones 'raras' con tu ordenador-, las amenazas de ciberdelincuentes controladas… así que todo irá bien, siempre que te mantengas en esa página y finalices la compra en el mismo sitio. En muchos casos, los criminales insertan falsos anuncios en webs de compra-venta para atraer a sus víctimas y que paguen por cosas que ni siquiera existen.

***CÓMO PUEDES EVITARLO** Haz caso omiso de anuncios o pequeñas ventanas que 'se abren' con ofertas irresistibles: puede tratarse de una trampa –si haces 'click' sobre ellas, te podrías estar descargando un virus-.*



FOTOGRAFÍA: WOLFGANGFOTO

PROGRAMAS 'ESPÍA'

Robar tus datos y toda la información que manejes en la red es el objetivo de estos programas silenciosos, que se ejecutan a veces enmascarados tras una App y que se instalan en tu dispositivo sin llamar la atención. Si tu ordenador está infectado, el ciberdelincuente tendrá acceso a todas las páginas por las que navegues, podrá hacer capturas de pantalla, saber tus claves controlando lo que teclees, captar imágenes y vídeos a través de la webcam o grabar sonido mediante el micrófono. Existen personas capaces de adueñarse de tu vida y sólo te darás cuenta cuando quieras acceder a tus cuentas con tus claves y éstas ya no sirvan porque alguien ha accedido y las ha cambiado. En definitiva, un hacker puede hacerse con el control de tu ordenador... ¡y de tu vida!

4 TUS COMPRAS, EN WEBS CONOCIDAS

Páginas como Airbnb, HomeAway y VRBO puede que no te suenen, pero se están convirtiendo en referentes de todo lo relacionado con temas de alquileres para las vacaciones... y las personas que las dirigen hacen enormes esfuerzos por proteger a sus usuarios.

CÓMO PUEDES LOGRARLO: ***Nunca te fíes de una entidad desconocida. Puedes comprobar la reputación de una web analizando los comentarios de los usuarios. Además, cualquiera de estas páginas debe tener una información de contacto; si tienes la más mínima duda sobre la 'legitimidad' de una de esas agencias, llámales. Mantener una conversación 'real' te mostrará si son de fiar.***

BUENA IDEA: ***Para comprobar la reputación 'online' de una web, puedes utilizar una herramienta de Google que analiza las amenazas de ciberseguridad de las páginas. Puedes acceder a ella tecleando: http://google.com/safebrowsing/diagnostic?site= seguido de la dirección de la página que quieres visitar. También puedes utilizar la herramienta Kaspersky Security Network -es gratis-, que usa bases de datos en la nube, actualizadas de manera constante, para analizar páginas web y programas y detectar cuáles pueden ser una amenaza.***

5 TELÉFONO 'DE ALTA SEGURIDAD'

Prácticamente toda nuestra vida está almacenada en nuestro teléfono y gracias a él tenemos acceso a correo, redes sociales, pagos y compras online. Nos ha facilitado mucho nuestro día a día al no depender de un dispositivo fijo para conectarnos a la red. Pero, al igual que haces con tu ordenador convencional, tu smartphone debe estar protegido contra ataques externos o por si lo pierdes.

CÓMO PUEDES EVITARLO: ***Utiliza aplicaciones de localización como 'Find my iPhone' o 'Administrador de dispositivos Android'. Recuerda que estas aplicaciones sólo funcionan mientras el teléfono esté operativo y conectado a Internet.***

6 NO PAGUES DESDE MÓVILES Y TABLETS

Estos tienen unas pantallas más pequeñas que las de cualquier ordenador y, además, según el navegador que uses, verás el contenido de las páginas web de forma diferente... así que muchas veces es difícil saber si estás usando una página segura mientras realizas un pago online. Lo ideal es pagar tus vacaciones desde tu ordenador.

CÓMO PUEDES EVITARLO: ***Si no te queda más remedio, protege tu tablet y/o smartphone con un paquete de seguridad móvil como los que comercializan conocidas compañías como Kaspersky, Norton Symantec, Panda o Eset -por un precio que oscila entre siete y 10 euros-. Se trata de programas que se encargan de chequear tu actividad para detectar cualquier software malicioso que tengas.***


PON A SALVO TODAS TUS CLAVES

Bastan unos pocos minutos conectado a una red wifi insegura para que un ciberdelincuente copie todas tus claves de acceso -al correo, a tus cuentas bancarias, a las redes sociales...-. Todo lo que haya sobre ti en Internet estará a disposición de los llamados 'blackhat hackers' que podrán robar el dinero de tus cuentas, invadir tu intimidad e incluso robarte la identidad, hacerse pasar por ti y convertir tu vida en una pesadilla. Así lo consigue:


7 PHISHING

El término proviene de la voz inglesa 'fishing' -pesca- y como si de indefensos peces se tratase, los usuarios se enfrentan a esta amenaza en forma de correo electrónico o páginas web donde se les requiere información sensible sobre sus cuentas bancarias o contraseñas.

EN QUÉ CONSISTE: ***El ciberdelincuente, llamado 'phisher' -pescador- se hace pasar, mediante estudiadas técnicas de ingeniería social, por una persona de confianza o un trabajador de la empresa que suplanta: por ejemplo, tu banco, diciéndote que necesitas renovar tus claves y que, para ello, debes facilitarles la antigua.***



FOTOGRAFÍA: BEN AND KAZ ASKINS



***QUÉ CURIOSO:* Esta técnica también ha sido utilizada para suplantar páginas de redes sociales, como ocurrió con la web MySpace en 2006, que sufrió un ataque que permitió redireccionar a una página falsa multitud de informaciones de sus usuarios.**

8 KEYLOGGERS

Es un pequeño programa instalado en un ordenador y que es capaz de memorizar todo lo que teclees, incluidas tus claves y códigos de acceso, ya sea la que pones cuando 'arrancas' el ordenador ya sean tus contraseñas de redes sociales, cuentas bancarias o correo electrónico. Este fraude es bastante común en lugares donde utilizas un ordenador que no es el tuyo, como por ejemplo en tu lugar de trabajo, en un cibercafé, en un hotel o aeropuerto...

***CÓMO EVITARLO:* Sencillo: procura no realizar operaciones 'sensibles' que puedan poner en riesgo este tipo de información en ordenadores que no sean de confianza.**

9 STEALERS Y USB DRIVES

Como bien indica su nombre son 'ladrones' -'stealers' en inglés-. ¿Tienes por costumbre decirle 'Sí quiero' a tu navegador cuando te sugiere guardar tus contraseñas? Pues es una forma de allanar el camino a los ciberdelincuentes que utilizan estas aplicaciones para robar datos sensibles como tus contraseñas y claves.

***CÓMO EVITARLO:* Si eres propenso a olvidar tus claves la solución te la dan administradores de contraseñas como KeePassX. Es preferible que no funcionen en la 'nube' -donde pueden sufrir más ataques-, sino que uses aplicaciones instaladas en el propio dispositivo. No te olvides limpiar las cookies y tu historial de navegación de vez en cuando.**

***QUÉ CURIOSO:* Una de estas empresas que gestionan tus contraseñas en la 'nube', llamada LastPass, sufrió este año un ciberataque que comprometió, no sólo las claves de acceso de sus usuarios, sino todas las contraseñas que alojaron.**

10 RANSOMWARE Y SMARTPHONES

Si eres usuario de páginas de descarga de contenidos o juegas con tu teléfono, debes estar prevenido contra el 'ransomware': un software malicioso que 'aparecerá' en tu ordenador informándote de que estás cometiendo un delito. Se harán pasar por una especie de 'policía cibernética', bloquearán tu ordenador, secuestrarán el disco duro y/o cifrarán tus archivos. Tu pesadilla será aún mayor cuando te digan que tendrás que pagar dinero a cambio de que tu ordenador 'sea liberado'.

***CÓMO EVITARLO:* Instala un buen antivirus así como un cortafuegos 'potente'. Hazlo también con tu smartphone y evita descargarte aplicaciones que no provengan de las tiendas oficiales.**

***QUÉ CURIOSO:* Es muy frecuente que, al pinchar un enlace de confianza, te 'salte' una publicidad engañosa -las llamadas 'pop ups'- que te avisa de un virus que acaba de infectar tu dispositivo. Te ofrecerán descargarte un estupendo antivirus de manera gratuita para limpiar tu 'smartphone'. ¡No lo hagas jamás!... se trata de un virus.**

IMPIDE QUE CONTROLEN TU VIDA DIGITAL

EVITA QUE SE APODEREN DE TU 'VIDA DIGITAL' HACIÉNDOSE PASAR POR TI EN REDES SOCIALES

La hacker, CEO de Wickr y organizadora de la DefCon en 2014, Nico Sell, nos da unas sencillas recomendaciones para mantener nuestra información a salvo y evitar lo que se llama 'suplantación de identidad digital':

Elimina tu fecha de nacimiento de tu perfil de Facebook. Tendrás que sobrevivir sólo con las felicitaciones de tus conocidos más cercanos o de aquellos que tengan suficiente memoria.

Rechaza que Twitter o Instagram muestren tu localización. Esta información es vital para los ciberdelincuentes, que la utilizarán para, con ayuda de técnicas de ingeniería social, saber dónde estás en cada momento. ¿Estás cenando fuera? Perfecto, tu casa está vacía…

Tapa todas las cámaras que vienen integradas en tus dispositivos: teléfono, portátil, televisión… Son fácilmente accesibles para un 'black hat hacker'.

Lee la letra pequeña sobre políticas de privacidad de aquellas aplicaciones y programas que instales en tus dispositivos. Son válidas a escala mundial y… ¡para siempre!

No proporciones tus datos a cualquier página que te los solicite. Quedarán para siempre en la red y los ciberdelincuentes se nutren de todos estos datos que encuentran en Google.

Usa tarjetas de crédito virtuales para proteger las verdaderas en caso de robo de tus datos online. Utiliza el servicio de empresas como NETELLER -http://www.neteller.com-.

CONSULTORIO

Cómo crear claves robustas y seguras; así puedes evitar que te espíen cuando navegas en Internet; ¿es seguro usar las tarjetas de pago contactless ...?



BUENA IDEA

CÓMO ELEGIR LA CONTRASEÑA MÁS SEGURA

FEDERICO LÓPEZ, CIUDAD REAL

Usa una diferente para cada servicio y recuérdalas con un sencillo truco de memoria

Los cibercriminales siempre se las ingenian para crear programas informáticos o virus que les permitan robar las claves de sus víctimas, normalmente para conseguir un beneficio económico. **Rafael Gómez-Lus, experto legal de Trusted Shops** -un sello de calidad para tiendas 'online'-, te da cinco consejos para crear contraseñas que realmente te protejan de los intrusos en tus perfiles y cuentas online:

#1 Crea contraseñas de, al menos, 10 dígitos -combinando letras, números y signos como '&' o '%'-. Nunca guardes tus contraseñas sin cifrar en el disco duro del ordenador, ni las dejes escritas en lugares que puedan ser vistos por otras personas.

#2 Intenta no introducirlas cuando uses ordenadores públicos, por ejemplo, los de cibercafés, hoteles, etc.

#3 Nunca envíes contraseñas por correo electrónico, ni respondas a un correo que te las solicita.

#4 Asegúrate de responder a la pregunta de seguridad con respuestas que sólo tú conozcas. Con la llegada de las redes sociales, los cibercriminales pueden conocer mucha más información sobre ti de la que crees. Es importante que cambies tu contraseña con frecuencia. No mantengas la misma más de 30 días.

#5 ¿Sabes que la contraseña "Contraseña" es una de las más populares? Por eso, es recomendable que no uses palabras procedentes del diccionario -es mejor 'que te las inventes'-.

Y, sobre todo, es conveniente que utilices una contraseña diferente para cada sitio web.

Regla de oro para crear contraseñas: Divídela en frases fáciles de recordar. Por ejemplo: "Laura tiene 2 perros negros y 3 gatos blancos". A continuación, reduce esta frase a las iniciales de cada palabra, lo que daría como resultado "Lt2pny3gb". Para incrementar aún más la seguridad, incluye caracteres especiales. En este caso, puedes sustituir "y" por "&", es decir:"Lt2pn&3gb".



¿Cómo puedo evitar dejar rastro al navegar por Internet? No me gusta que alguien descubra todas las webs que visito.

Lidia Sánchez, Málaga

La forma más fácil es activar en tu navegador una opción llamada 'ventana de incógnito'. Se trata de un sistema que utilizan los hackers y miembros de los cuerpos de seguridad para investigar ciertas actividades y a determinados sujetos. La ventana de incógnito hace más difícil que los responsables de una web sepan realmente quién les está visitando. Pero los expertos aseguran que, si realmente quieres acceder a una web sin que ésta sepa quién eres, lo mejor es que utilices lo que se conoce como navegadores específicos o páginas 'proxy'. Con ellos, podrás encriptar tus datos, de forma que ocultes tu dirección IP y sólo sea visible la del proxy web. Para conseguir la máxima seguridad, podrás crear una cadena de proxy webs enlazadas, que hará imposible para cualquier página saber que eres tú quien está 'al otro lado'.

Puedes configurar un proxy manualmente o con herramientas automáticas como JAP -'Java Anonymous Proxy'-, que hace que todos sus usuarios naveguen con una misma dirección IP, de forma que cualquiera que utilice esta herramienta para moverse por Internet, irá dejando ese mismo 'rastro'. Puedes instalar JAP gratis desde http://anon.inf.tu-dresden.de/win/download_en.html

Juan José Altea, One Magazine



¿Me puedo fiar de las direcciones 'acortadas' que se usan en redes sociales como Twitter? ¿Cómo puedo saber si es seguro 'pinchar' en una de ellas?

Montse Mateu, Barcelona

En Internet, existen servicios gratuitos -owly, google shortener...- que reducen la longitud de las direcciones web para que ocupen menos en los mensajes de redes sociales. El problema es que los ciberdelincuentes se valen de los enlaces acortados para redirigir a los usuarios a sitios maliciosos, ya que dan menos pistas sobre la web a la que nos van a llevar. De hecho, según un estudio realizado por la empresa Web of Trust, entre el 5% y el 10% de los enlaces acortados redirigen a los usuarios a sitios de phishing, spam o descarga de malware. Para detectarlos, existen servicios gratuitos de verificación, como www.knowurl.com o Longurl.org, que te permiten introducir una dirección acortada para saber si el sitio al que te llevaría es de fiar.

Oficina de Seguridad del Internauta -OSI-



¿Cómo puedo saber si me han robado datos personales?

José María Medina, Madrid

Existe una web, -https://haveibeenpwned.com- que se dedica a recopilar de forma altruista las listas de datos que los ciberdelincuentes han robado de páginas como la plataforma de contactos Adult Friend Finder. También es capaz de decirte si tu servidor de correo ha sido hackeado: basta con que introduzcas tu email para que, mediante un color -rojo o verde-, te diga si es mejor que cambies tus claves. Además, si eres administrador de un dominio web puedes solicitar que esta página te indique cuántas de sus cuentas han sido comprometidas.

José Manuel Vera, One Hacker



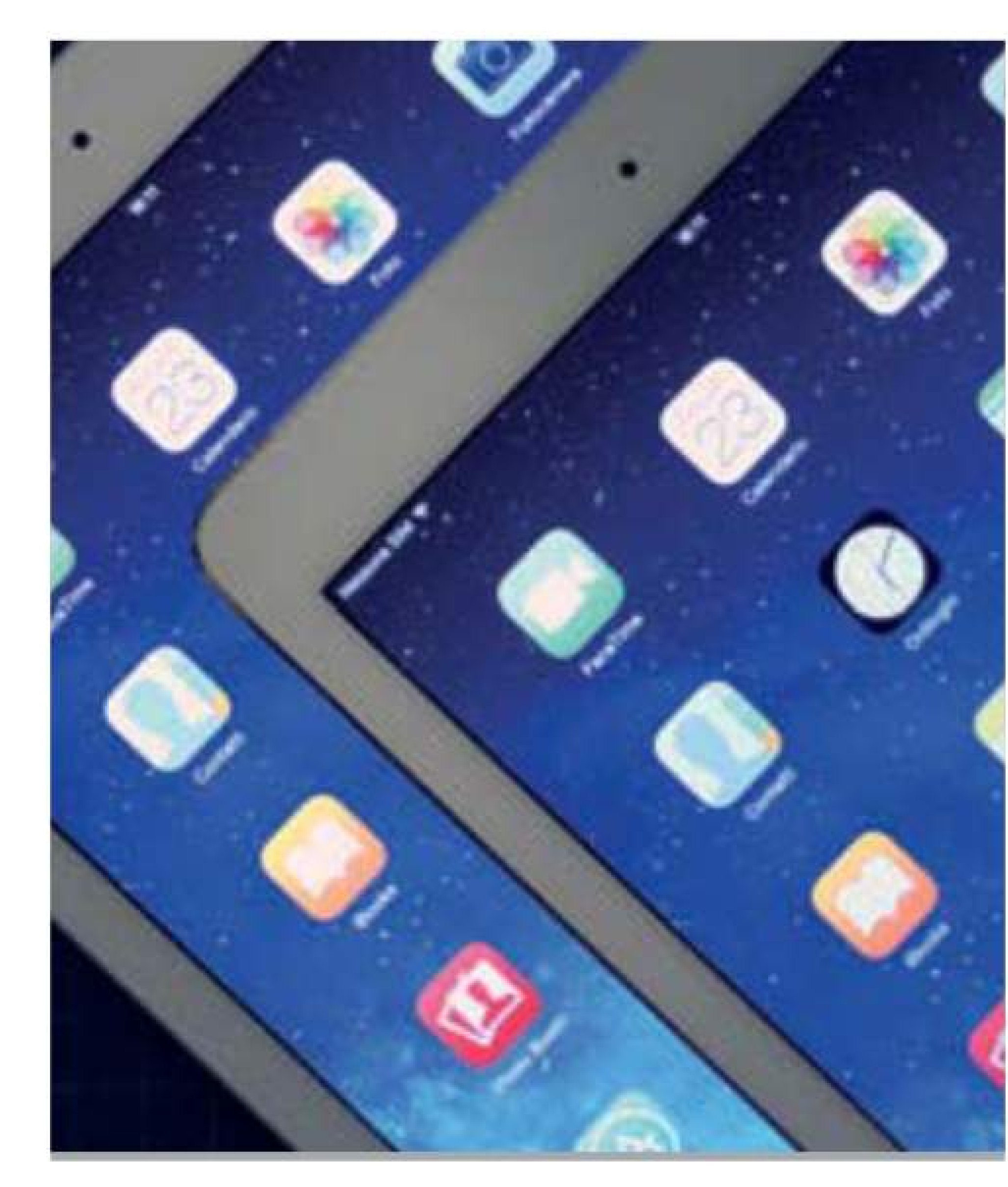
¿Qué es el egosurfing?

Alicia Serranillo, Burgos

Es la práctica de buscarte a ti mismo en Internet, la cual te permitirá conocer la imagen que proyectas en la red.

Esta imagen está formada por lo que tú hayas ido publicando -perfiles en redes sociales, comentarios, etc.- y por lo que otros hayan publicado sobre ti. Es bueno practicar el egosurfing de vez en cuando, para saber qué se dice sobre nosotros, cómo se dice y quién lo cuenta. Los resultados obtenidos constituirán parte de lo que se conoce como 'identidad digital'. Es decir, el perfil que cada persona tiene en Internet.

David Noriega, One Hacker



¿Es cierto que los dispositivos Apple no tienen virus?

Ricardo Casamayor, Logroño

No es cierto. A priori, puede que a los criminales no les compense crear malware para sólo un 10% de los dispositivos móviles -los que usan el sistema operativo iOS de Apple-, pero en los últimos meses se ha incrementado el número de ciberamenazas contra dispositivos de esta marca. Entre otras, el troyano XcodeGhost ha infectado a más de 300 aplicaciones de la tienda oficial de Apple, que ya han sido utilizadas por 210 empresas. Además, investigadores de la empresa FireEye han descubierto otra nueva amenaza en miles de aplicaciones de la App Store, mediante la cual el atacante podría acceder a información confidencial.

Josep Albors, director Laboratorio Eset.

Envía tu pregunta a:
ONE Hacker
e-mail: onemagazine@grupoateneasn.es





Noemí Brito

MIEMBRO DEL COMITÉ OPERATIVO DEL DATA PRIVACY INSTITUTE DEL ISMS FORUM

¿EUROPA PROTEGE TUS DATOS?

La principal misión de las autoridades que se encargan de la protección de datos es velar por el cumplimiento de la legislación en esta materia, a pesar de que los ciudadanos y las empresas tienen la falsa percepción de que su labor se centra en abrir procesos sancionadores y poner multas.

Estas autoridades también llevan a cabo importantes funciones en materia de concienciación, información, atención al ciudadano, etc. Y es que no es fácil para estos organismos convencer a la sociedad de que la privacidad “no es una moda pasajera”, sino algo que forma parte de lo digital, en la que el ciudadano juega un papel muy importante.

Asimismo, el actual contexto mundial, los constantes flujos globales de información, así como los últimos incidentes terroristas, implican nuevos desafíos para la protección de la privacidad por parte de las autoridades. Estas están abocadas a adoptar un nuevo papel en la sociedad, quizás mucho más activo.

En este ámbito, la reciente Sentencia del Tribunal de Justicia de la Unión Europea del 6 de octubre de 2015 destaca por darle más importancia a las competencias de las agencias nacionales, al declarar que éstas deben operar con total independencia, sin tener que verse limitadas por las decisiones de la Comisión Europea.

Esta sentencia supone un importante espaldarazo a las autoridades de control –las agencias nacionales de protección de datos–, que deben aprovecharlo para impulsar su actuación, haciendo cada vez más partícipes en estos procesos a ciudadanos, empresas y profesionales, y reforzando la coordinación y cooperación entre las mismas, tal y como apunta el próximo Reglamento Europeo de Protección de Datos.



¿Cómo puedo saber fácilmente que mi móvil no está infectado?
Miguel Ángel Muñiz, Madrid
En el mercado existen diferentes tipos de software -por unos 10 euros- para análisis de móviles, que chequearán tu dispositivo y te indicarán si está infectado. Si no te quieres gastar dinero, en la web del Incibe -www.incibe.es- encontrarás un software gratuito, llamado CONAN Mobile, que ayuda a mantener los dispositivos móviles Android a salvo de amenazas. CONAN Mobile te alertará, por ejemplo, si una aplicación que tienes instalada en tu móvil realiza una conexión a un destino potencialmente peligroso. Si quieres obtener más información sobre medidas de seguridad en telefonía móvil, consulta el Informe de Amenazas del CCN-CERT -Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional-, escaneando este código QR.
Borja G. de Sola, One Hacker



FOTOGRAFÍA: AUTOR BROCK CRAFT - THATBROCK AT EN.WIKIPEDIA

LA CENTRALITA TELEFÓNICA... NACIÓ FRUTO DE UN ¡CIBERATAQUE!

TUXOTRON / CYBERHADES.COM

A finales del siglo XIX, las centralitas telefónicas estaban controladas por el factor humano. Esto tenía cosas buenas, como la toma de decisiones, el toque personal, etc., pero también sus cosas malas: era lento, costoso, se cometían errores, cotilleos... Era sólo cuestión de tiempo que el operador telefónico acabara desapareciendo de esta ecuación y fuera una máquina la que conectara al que llamaba con el destinatario de forma totalmente automática. Como la mayoría de los inventos en nuestra vida, estos aparecen como respuesta a alguna necesidad. En este caso, fue a finales de 1880, cuando el dueño de una funeraria, Almon Strowger, en Kansas City, Missouri, EE.UU., empezó a notar una caída importante en la actividad de su negocio. Y no era, precisamente, porque la gente no se muriese, sino porque, según sus sospechas, la mujer del dueño de otra de las funerarias de la misma ciudad trabajaba como operadora telefónica y todas las llamadas que recibía preguntando por la funeraria, las mandaba al negocio de su marido. Esto es lo que hoy en día llamaríamos 'Man in the Middle' -Hombre en el medio o, más bien, 'Woman in the Middle'-, un ataque en el que un intermediario modifica un mensaje entre dos partes sin que ninguna se entere de ello.

Strowger, evidentemente, tenía un problema y varias opciones para solucionarlo: denunciar a la compañía de teléfonos o a la operadora, hablar con la funeraria de la competencia, etc., pero nada de eso cortaría el problema de raíz: hacer desaparecer el factor humano de los conmutadores telefónicos, posiblemente la solución más elegante. En 1888, a Strowger se le ocurrió la idea del conmutador Strowger -Strowger switch- y, tres años más tarde, patentó el Conmutador Telefónico Automático -Automatic Telephone Exchange-. Ese mismo año, creó Strowger Automatic Telephone Exchange Company, una empresa para la comercialización de su conmutador mecánico telefónico.

Dicha máquina permitía la llamada entre usuarios -conectados en la misma centralita- sin necesidad de la intervención humana. En su versión original, el teléfono de los usuarios sólo disponían de tres botones: centenas, decenas y unidades. Si un usuario quería llamar al número 531, pulsaba cinco veces el botón de las centenas, tres veces el de las decenas y una vez el botón de las unidades.

El primer conmutador de Strowger se instaló en 1892 en La Porte, Indiana -EE.UU.-, con 75 usuarios iniciales -y con capacidad para 99-. Esta fue “la primera gran evolución” de la centralita telefónica y quizás las más importante. En 1916, la compañía Bell empezó a usar los conmutadores de Strowger fabricados por Automatic Electric -empresa en la que se convirtió Strowger Automatic Telephone Exchange Company- y, en 1926, empezó a fabricar los suyos propios, llamados sistemas paso-a-paso -step-by-step-.

INTERNET PARA TODOS

MÁS DE MEDIO MUNDO YA ESTÁ CONECTADO

+ Info

Ángel Avilés 'Angelucho'
EDITOR DE "EL BLOG DE ANGELUCHO"

Como miembro del colectivo 'X1RedMasSegura' son muchos los talleres en los que he participado intentando abrir los ojos a padres y educadores sobre los peligros a los que se enfrentan nuestros hij@s en la red, así como a personas mayores, víctimas de la conocida como brecha digital; en resumen, a individuos muy vulnerables cuando se enfrentan a un medio en el que se potencian las incapacidades. Una labor a la que también se dedican la mayoría de los congresos de seguridad informática, de Hacking que, en paralelo a las actividades técnicas, ofrecen talleres para concienciar a un público no técnico. Con ello rompen el falso concepto de asociar el término 'Hacker' a ciberdelincuente o quinqui. Una pasión con la que quiero aportar mi grano de arena en **One Hacker** dando a conocer los peligros a los que tod@s hacemos frente en nuestra 'cibervida'.

Y, para ello, la mejor forma es comenzar por el principio. Internet nos ofrece un maravilloso mundo de posibilidades. Sin embargo, se trata de un concepto vinculado directamente a la informática y los ordenadores. **Ello supone un problema para los "inmigrantes digitales"**, que consideran que acceder al ciberespacio está limitado a quien maneje a la perfección la informática.Las nuevas tecnologías han modificado los hábitos de socialización, hemos cambiado las tertulias en cafés y bares por conversaciones en la distancia a través de las redes sociales. Incluso hemos transformado las comunicaciones persona a persona por los contactos, hasta con gente que no conocemos, a través del difuso mundo del ciberespacio.

Internet ha cambiado el modo en el que comprendemos las comunicaciones y el mundo. Está claro que, desde la imprenta, es el mejor vehículo de difusión cultural conocido. **Desde su evolución a lo que se ha dado en llamar Web 2.0, las posibilidades se han multiplicado**, ya que ahora es un medio donde el usuario no es pasivo, sino que puede interactuar con otras personas y crear sus propios contenidos, al contrario que los medios de comunicación que existían con anterioridad. ¿La clave de su éxito? Es un 'producto' que reúne las tres 'B' de bueno, bonito y barato, además de una forma rápida y eficaz de comunicación inmediata con nuestro interlocutor.

Desde 2010 la Web 2.0 ha cobrado un protagonismo especial, con cada vez mayor presencia en la forma de inter-relacionarse los internautas. Según datos del Instituto Nacional de Ciberseguridad -INCIBE-, a finales de 2011 había cerca de 1.800 millones de usuarios de Internet en todo el mundo. En la actualidad, podemos afirmar que las redes de interacción social se han convertido en uno de los elementos de Internet más difundidos, ya que ofrecen a sus usuarios un lugar común para desarrollar comunicaciones constantes. Esto es posible gracias a que los usuarios pueden acceder a Internet a través de su ordenador, móvil, tablet... Una ventaja que también han aprovechado las empresas y el márketing para interactuar con el consumidor.

Hasta ahora, sólo he hablado de algunas de las bondades de Internet -enumerarlas todas requeriría miles de páginas- porque **estoy convencido de que el 99% de lo que entendemos por Internet doméstico son bondades.**

Lamentablemente queda un pequeño 1% que representa la cara 'B' de la red, los peligros de Internet que iré desgranando en **One Hacker** para convenceros de que "en Internet, nosotros somos nuestra mayor vulnerabilidad, pero también somos nuestro mejor antivirus".

¡¡Nos vemos en la Red!!



Ángel es autor del libro "X1Red+Segura Informando y Educanco V1.0" y co-autor de la obra "¡Atención mamás y papás!" -ya a la venta-. Además, pertenece al Grupo de Delitos Telemáticos de la Guardia Civil.

EL DESCONTROL
DEL INTERNET DE LAS COSAS



Josep Albors
DIRECTOR DEL LABORATORIO ESET

Más de uno estará harto de escuchar hablar del cacareado Internet de las Cosas y de sus, supuestamente, múltiples bondades. No cabe duda de que los avances realizados en los últimos años han permitido a dispositivos de todo tipo conectarse entre sí y a Internet para hacernos la vida más fácil.

Parece una situación idílica, ¿verdad? Ahora mismo, desde nuestro smartphone podemos gestionar aspectos tan variopintos como bajar o subir las persianas de casa, revisar si nos queda poca leche en la nevera o asegurarnos de tener un café calentito al levantarnos. Todo de color de rosa y pensado para que nuestro día a día sea más llevadero o al menos, así sería si cada fabricante no hubiese tirado por donde más le hubiese convenido, ahorrándose gastos asociados en seguridad.

EL INTERNET DE LAS COSAS… VULNERABLES

Parémonos a pensar, ¿quién ha actualizado alguna vez su Smart TV?, ¿y la nevera?, ¿y aquella cámara IP que se compró para vigilar al bebe recién nacido? Las respuestas a cualquiera de estas preguntas harían que cualquier evangelizador en seguridad pensase en retirarse a meditar a algún recóndito lugar, al comprobar como casi todos los usuarios hacen caso omiso a sus consejos.

El problema es que si ya cuesta conseguir que actualicemos algo tan básico como nuestro sistema operativo y las aplicaciones que utilizamos a diario -algo relativamente sencillo, aunque solo sea para evitar los parches de seguridad que aparecen en las pantallas-, pedirle a un usuario medio que revise su Smart TV o router para comprobar si hay alguna actualización disponible es tener mucha fe.

Poca gente es consciente de que el nuevo dispositivo conectado que acaba de adquirir puede suponer un riesgo para su privacidad o los datos que almacen. Algunos, incluso, han pensado que dotando de conectividad a un juguete como la Barbie van a conseguir que sus hijos interactúen de forma más personal con la rubia más famosa. Poco les importa que pueda comprometer la privacidad de alguien tan vulnerable como un niño.

RIESGOS PRESENTES Y FUTUROS

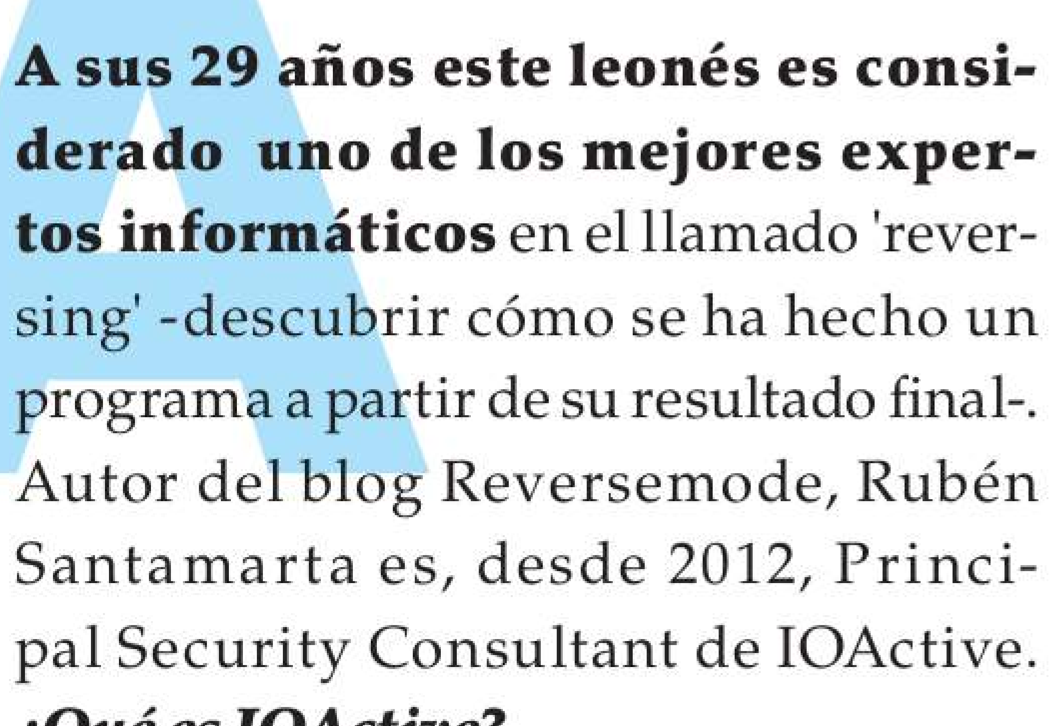
Decir que un coche puede ser hackeado ya no sorprende a nadie desde que varios investigadores consiguieron hacerse con el control de varios modelos, incluso de forma remota. Por desgracia, ni los usuarios ni la industria parecen preocuparse por una amenaza que es real. El problema es que en un coche existe un riesgo que traspasa el mundo digital y nos afecta en el mundo real. A nadie le gustaría comprobar en sus carnes las consecuencias de desactivar los frenos cuando circula por una autopista, pero es una posibilidad real. Y, cuando hablamos de amenazas para la salud, no podemos olvidar los múltiples dispositivos médicos que actualmente incorporan conectividad y la posibilidad de acceder remotamente a ellos. Pensemos, por ejemplo, en modelos de marcapasos o bombas de insulina que incorporan la posibilidad de ser gestionados a cierta distancia por otros dispositivos que permiten ajustar sus valores. Para terminar de rizar el rizo, existen incluso rifles que incorporan miras de precisión que podemos conectar a nuestro Smartphone. Alguien debio pensar que se trataba de una función muy útil grabar el momento en el que se acierta a la presa pero también supone un riesgo si alguien accede a esa mira y alterar su funcionamiento.

¿EXISTE UNA SOLUCIÓN A ESTE DESCONTROL?

Como usuarios tenemos bastante limitada las posibilidad de actuación, puesto que dependemos de que los fabricantes publiquen actualizaciones que solucionen los problemas que pudieran aparecer en el software encargado de manejar estos dispositivos. Si trasladamos el problema al lado de los fabricantes, veremos que estos están más interesados en lanzar dispositivos de todo tipo con capacidades de conexión cada cierto tiempo que en protegerlos de posibles ataques o incluso solucionar problemas existentes en versiones anteriores. Hace falta que se establezca una fuerte normativa para que los controles de calidad se amplíen a la seguridad lógica y se impongan sanciones a aquellos fabricantes que no la cumplan. Pero, como siempre, hay muchos intereses de por medio...

RUBÉN SANTAMARTA

IOACTIVE SE HA HECHO FAMOSA POR HABER DEMOSTRADO QUE ALGUNOS COCHES SON HACKEABLES. UNO DE SUS MÁXIMOS RESPONSABLES EN SEGURIDAD NOS HABLA DE LO QUE LE PREOCUPA DEL CIBERESPACIO.



A sus 29 años este leonés es considerado uno de los mejores expertos informáticos en el llamado 'reversing' -descubrir cómo se ha hecho un programa a partir de su resultado final-. Autor del blog Reversemode, Rubén Santamarta es, desde 2012, Principal Security Consultant de IOActive.

¿Qué es IOActive?

Somos una empresa de hackers... tanto cultural como técnicamente. Nos apasiona lo que hacemos. Con sede en Seattle -EE.UU.- ahora acabamos de abrir un laboratorio en Madrid porque nos permite tener un centro de referencia en seguridad hardware para EMEA -Europa, Oriente Próximo y África- similar al que ya tenemos en Seattle -EE.UU-. Además, así apostamos por el talento español.

¿Cuál es vuestro punto fuerte?

Somos buenos investigando la seguridad de sistemas críticos como satélites, sistemas de control industrial, aplicaciones móviles, cajeros de bancos o coches. Ofrecemos servicios que van desde el análisis de todo tipo de sistemas hasta de los llamados 'smart meters' –contadores digitales que se usan para, por ejemplo, medir el consumo de luz, agua... etc-.

¿Qué te preocupa del ciberespacio?

Como persona, la exposición de nuestros datos y falta de privacidad; como empresa, el robo de propiedad intelectual. Para cualquier país, un ciberataque, además de daños a la economía, conlleva la pérdida de confianza de sus ciudadanos y sensación de inseguridad.

¿De qué depende que no suframos ciberataques?

De lo importante que seamos para el atacante. Si no tienes nada interesante para nadie, estás a salvo. A no ser que vivas en el bosque y te hagas amigo de un árbol, es probable que en algún momento de tu vida seas objetivo de un ciberataque, ya sea generalista o más adaptado a tu perfil.

Cómo saber si un móvil es seguro...

No hay trucos para eso... excepto tener un poco de sentido común. Hace poco, en unos grandes almacenes, me encontré con un teléfono en exposición que todavía tenía los datos y fotos de sus anteriores dueños. Si cambias algo después de comprarlo... ¡no olvides borrar tus datos!


¿Qué le pides a los políticos?

Que no se criminalice la curiosidad y el compartir el conocimiento. En términos generales, creo que la mayoría de partidos políticos podrían alcanzar acuerdos en materia de ciberseguridad sin tantos problemas como en otros ámbitos. Creo que fomentar el aprendizaje sobre seguridad informática entre las nuevas generaciones es bastante importante.

Para ser el mejor hacker...

Lee mucho, todo y más. Practica lo aprendido y no busques convertirte en una referencia en ciberseguridad... Si crees que tienes ese perfil y quieres trabajar en IOActive...-risas- pues envíarnos tu currículum a careers@ioactive.com-.

"HAY QUE FOMENTAR LA SEGURIDAD INFORMÁTICA ENTRE LAS NUEVAS GENERACIONES"


IOActive
IOActive
IOACTIVE OPENS MADRID LAB
IOACTIVE MADRID HARDWARE RESEARCH LAB

APRENDE A PROTEGER TU WIFI



Las redes inalámbricas wifi nos han cambiado la vida, al ofrecernos la posibilidad de conectarnos a Internet -utilizando nuestro ordenador, móvil o tablet- sin necesidad de cables. Sin embargo, muchas de esas wifi también suponen un riesgo evidente, ya que si no están bien protegidas -ya sea la que tienes en casa o a la que te conectas en cualquier lugar público- pueden suponer toda una puerta de entrada para que un ciberdelincuente nos robe información, datos, fotos y cualquier tipo de archivo. Aprende cómo evitarlo.

CÓMO EVITAR QUE TE PIRATEEN EL WIFI

Que alguien se conecte a Internet utilizando tu Wifi puede suponerte algo más que la incomodidad de que tu conexión vaya más lenta: un criminal podría usarla para hacerse pasar por ti y cometer algún delito. Para evitar problemas, te enseñamos a restringir su acceso a cualquier extraño.

1 **Configura el router.** En la mayoría de estos aparatos podrás acceder al panel de control del router utilizando tu navegador de Internet y escribiendo los números 192.168.1.1 en la barra de direcciones. También necesitarás la clave de administración para entrar a la configuración del router. Ésta viene con el kit de instalación en una pegatina -o en la documentación adjunta-. En caso de no encontrarla pregúntasela a la compañía que te da el servicio.

2 **Protocolo seguro.** Para conocer qué protocolo utiliza, lo primero es acceder a la configuración del router. Si no sabes cómo hacerlo, puedes consultar el manual o buscar información sobre tu modelo en Internet –escribe su nombre en cualquier buscador-. El router debe incorporar, al menos, el protocolo WPA entre sus medidas de seguridad –lo dirá en el folleto de datos técnicos-. Si no encuentras estas siglas deberás actualizarlo.

3 **Cambia el protocolo.** Elige el sistema de seguridad más avanzado: el WPA2- PSK. Busca en el apartado 'opciones de seguridad' para configurar un sistema de cifrado o encriptación de este tipo. No es inexpugnable... pero sí muy seguro.

4 **Reemplaza la contraseña por defecto.** En el panel de control establece una clave de acceso robusta a la red Wifi. Debe tener, al menos, 12 caracteres incluyendo mayúsculas, minúsculas, números y símbolos. ¿Un truco? No tiene que poderse pronunciar en ningún idioma, explica Almudena Alcaide del Deloitte CyberSoc Academy. Esta nueva clave sustituirá a la que viene preconfigurada por defecto en el aparato –la verás en una pegatina en su parte inferior-.

5 **Modifica el nombre de la WiFi o SSID.** Normalmente, el SSID -o nombre de la red- viene definido por defecto. Éste debe ser sustituido por uno que no sugiera cuál es nuestro operador y que no guarde relación con la contraseña de acceso a la red. Así nadie sabrá qué tipo de WiFi es ni te podrán identificar –por ejemplo, si un vecino sabe que la tienes contratada con una compañía concreta-. ¿Un consejo? Puedes incluso configurar el router para que no emita el nombre del WiFi -siendo, en principio, ilocalizable para el gran público-.

6 **Modifica la contraseña para acceder a la configuración del router.** Normalmente vienen por defecto -"1234" o "admin"-. Conviene sustituirla para evitar que si alguien logra conectarse, pueda configurar el router a su antojo.

! Si te vas de vacaciones es recomendable desconectar el router. Además de ahorrar electricidad evitarás que alguien se intente conectar a él –igual con malas intenciones-.

7 **Desactiva la opción WPS** (WiFi Protected Setup) "Esta característica permite que un equipo se conecte a la WiFi utilizando un código temporal que simplifica todo el proceso de "conexión" de un nuevo equipo", explica un conocido experto en ciberseguridad. "Por desgracia, las implementaciones de muchos routers no detectan los ataques de fuerza bruta –obtener una clave probando todas las combinaciones posibles hasta encontrar aquella que permite el acceso- y en unos minutos están en tu red WiFi. Así que desactívalo y evita estos ataques de un tirón".



¡OJO AL DATO!

¿Usan los criminales tu WiFi para atacar grandes empresas?

Los ciberataques más habituales contra organismos y compañías son los llamados de 'denegación de servicio'. Consiste en 'tumbar' una web enviándola de forma simultánea millones de peticiones. Para ello se colonizan, con virus informáticos, millones de ordenadores que pasan a estar bajo el control del atacante dentro de lo que se llama 'red zombie'. Si quieres detectar si tu ordenador está infectado descárgate la herramienta de análisis AntiBotnet del Instituto Nacional de Ciberseguridad –Incibe- a través de su web ww.incibe.es



JULIO VIVERO
GMV

LE APASIONA CÓMO INTERNET ESTÁ CAMBIANDO EL MUNDO Y, COMO JEFE DEL ÁREA DE CONSULTORÍA E INFRAESTRUCTURAS DE GMV, TRABAJA PARA HACER LA RED MÁS SEGURA. PARA ELLO DESARROLLA TECNOLOGÍAS COMO ATALAYA, CHECKER O ARKANO, QUE PARECEN SACADAS DEL MUNDO DE LA CIENCIA FICCIÓN... PERO YA SON UNA REALIDAD.

Cada vez estamos más conectados...

Sí. Nuestra vida depende de Internet. Realizamos las compras online, pagamos impuestos, buscamos pareja... incluso nos reunimos sin vernos. Antes hablábamos por teléfono; ahora nos enviamos mensajes... y lo hacemos sin pensar en los peligros que corremos. Por ejemplo, la foto que publicamos en nuestro perfil de WhatsApp o la frase que identifica nuestro estado puede dar mucha información a delincuentes que quieran saber de nosotros y les basta con conseguir nuestro número de teléfono para acceder a nuestra vida. Tampoco somos conscientes de que, al navegar por Google –sobre todo si tenemos una cuenta Gmail–, nuestras búsquedas quedan registradas. Y, si lo hacemos desde el móvil, podemos dejar rastro hasta de los lugares en los que hemos estado. Para evitarlo, tenemos que entrar en la cuenta de Google -https://account.google.com- y borrarlos. Nada es gratis: en realidad, lo que hacemos en Internet es pagar con datos.

Qué te apasiona y qué te da respeto...

Me fascina la velocidad con la que cada día aparecen nuevas tecnologías que cambian nuestra forma de vida. En cambio, me impone respeto la pérdida de privacidad que en muchas ocasiones éstas conllevan. Por ejemplo, los últimos modelos de contadores de luz –los llamados 'smartmeters'– almacenan información de nuestro consumo hora a hora. Si un delincuente tuviera acceso a ellos, sabría cuando estamos en casa, cuándo no... e incluso qué aparatos usamos y a qué hora, al comprobar la cantidad de energía consumida. Y lo que es peor, podrían usar esta información para entrar a robarnos. Lo que hacemos en el mundo virtual suele tener consecuencias en el mundo físico.

Nombra tres tecnologías que parecen ciencia ficción, pero son reales

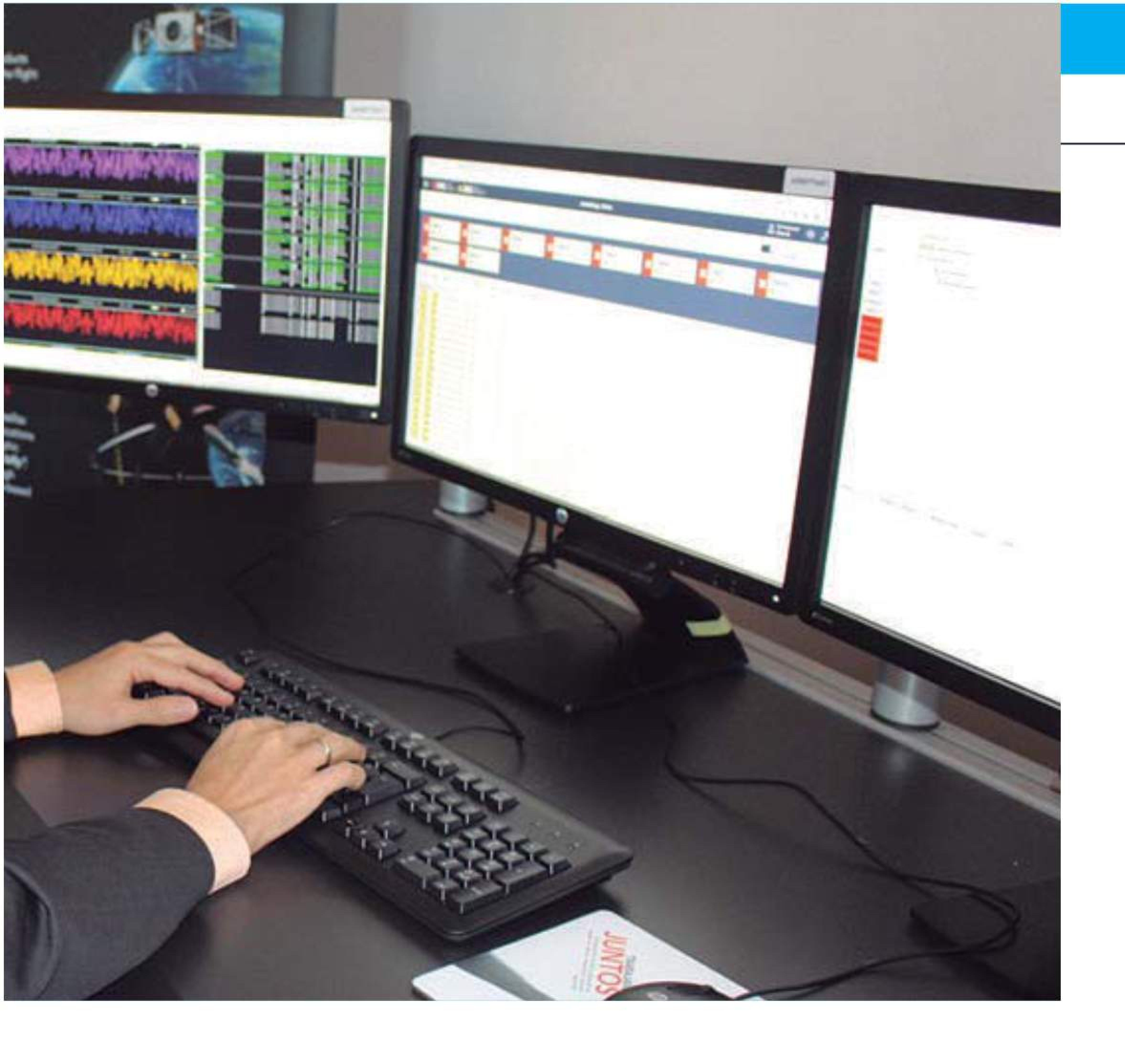
1 La primera es un proyecto increíble del Instituto Tecnológico de Massachusetts –MIT–. Se llama RF Capture y, mediante sensores y una red wifi, permite saber quién está detrás de una pared y si se encuentra bien. Está pensada para controlar el estado de personas mayores que viven en una casa, pero evidentemente también tiene muchas aplicaciones civiles y militares.

2 La segunda tecnología que me gustaría mencionar es el proyecto Oxford de Microsoft. Su tecnología de reconocimiento facial permite averiguar cuáles son las emociones de una persona a través de la expresión de su cara. Gracias a esta tecnología, en un aeropuerto se podría detectar a personas que den muestras de nerviosismo porque lleven drogas o explosivos.

3 Por último, la gran tecnología que me maravilla más es la inteligencia artificial. Algunos científicos, como Stephen Hawking, alertan de que con ella las máquinas se podrían sublevar. Pero actualmente, la inteligencia artificial nos permite analizar todos los datos que hay en el ciberespacio –incluso en la Deep Web, la red a la que accede a través de pasarelas especiales no visibles desde el Internet 'normal'– y saber cuándo se va a producir un ciberataque contra una empresa, un país, la banca... En GMV hemos desarrollado Atalaya, un producto que, gracias a su 'inteligencia', aprende de su experiencia para buscar amenazas, vulnerabilidades, fraudes, etc.

La clave para evitar ciberataques...

Contar con tecnologías como Atalaya de GMV. Se trata de lo último en ciber- inteligencia –el área de mercado que más va a crecer en este sector–. Para garantizar la máxima seguridad no basta con



responder a un ataque, lo determinante es poder conocer a tu enemigo e ir un paso por delante de él. Imagínate que los bomberos supieran dónde se va a producir un fuego y estuvieran allí con antelación. Esa es la clave para evitar ataques, tener la capacidad de anticiparnos.

¿Cómo ayudáis desde GMV a que el mundo sea más seguro?

Somos expertos en identificar los riesgos que más pueden afectar a nuestros clientes en el ámbito de la ciberseguridad. Entre nuestros puntos fuertes destacaría el desarrollo de soluciones informáticas a la carta para problemas concretos que afectan a la ciberseguridad del cliente que no tiene la capacidad de resolverlos por sí solo. Y es que los retos forman parte del ADN de GMV. Entre las tecnologías de las que estamos más orgullosos destacan Checker, pensada para proteger a los cajeros automáticos de ciberataques; Codelogin, un software para autenticación de personas con doble identificación y doble canal para hacer transacciones seguras, incluso las realizadas desde el móvil; y Arkano, un producto que controla el acceso a los datos incorporando mecanismos criptográficos en ellos. Arkano está pensado para cifrar documentos de uso diario, como los correos electrónicos o los archivos presentes en las redes Intranet de las empresas. El cifrado se realiza "extremo a extremo", es decir, se controla que ningún intermediario o administrador de sistemas pueda acceder a los datos.

¿Qué es lo que menos se conoce de la actividad de GMV en ciberseguridad?

Diría que el gran abanico de servicios que ofrecemos y nuestra capacidad para desarrollar productos a la carta. Contamos con experiencia en ámbitos tan diversos como la defensa, la medicina, el espacio, el transporte, en los sectores público y privado… De hecho, hemos puesto en marcha un sistema que nos permite identificar tecnologías emergentes que nacen sin la seguridad adecuada, como la nube, las ciudades inteligentes, el Big Data, etc. El 10% de los beneficios de la compañía se destina a proyectos de I+D+I que evalúa un comité específico de entre todos los presentados por compañeros de GMV.

¿Qué os diferencia del resto?


Además de que siempre aceptamos los retos porque la innovación forma parte de nuestro ADN no buscamos el beneficio a corto plazo. Somos una empresa que da pasos firmes y seguros conscientes de que el éxito de la compañía está en el de nuestros clientes, pensamos en el largo plazo. GMV nació hace más de 30 años apostando por el talento y la calidad, dos razones por las que nuestro cliente no es ocasional, le acompañamos durante años en su crecimiento... Le ayudamos en sus problemas del día a día protegiendo su negocio.

Los ataques más graves en 2016…

Serán los llamados APTs –Ataques Persistentes Avanzados–. Son ciberataques que pasan desapercibidos para las empresas y que roban su información crítica llegando a suponer su quiebra. Los atacantes a los que nos enfrentamos forman parte de grandes grupos, muy organizados y con todo tipo de recursos. Afortunadamente, productos como Cheker ayudan a combatir estas amenazas, ayudando a las entidades financieras -bancos fundamentalmente- a controlar el software que se ejecuta dentro de los cajeros automáticos de su red, de tal forma que sólo el software conocido y permitido por la entidad pueda ejecutarse dentro del cajero. Pero no hay que olvidar que el punto más crítico de la seguridad son las personas: los mayores ataques siempre se producen por descuidos –o malas intenciones–-.

¿Qué es lo más curioso que hayáis hecho en ciberseguridad en GMV?

Entre nuestros clientes figuran muchos organismos que tienen la seguridad como prioridad, por citar algunos más conocidos, Europol o la Agencia Espacial Europea, y hay muchos proyectos que destacaría. Pero por citar uno, el análisis de riesgos de ciberseguridad que realizamos para la ESA. Les hemos formulado una serie de recomendaciones a la hora de controlar los riesgos para los diferentes tipos de misiones espaciales.



ROBOTS • DRONES • GADGETS STAR WARS • GAFAS VR

Se acabaron los típicos regalos de cumpleaños; si quieres impresionar a amigos y familiares, opta por un gadget de la próxima generación. Los hay sorprendentes, prácticos, originales... y, algunos, que sólo buscan llamar tu atención: en todo caso, estos son los 32 que te recomendamos. También preguntamos a expertos por su seguridad. // **Texto: José M. Vera / D. Noriega /**



LOS MEJORES DRONES PARA EL OCIO

Está prohibido volarlos al aire libre sobre personas o en ciudad y recuerda que para uso profesional tendrás que disponer de un título específico -y cumplir unas normas de seguridad-. // **Texto: D. Noriega**



1 AR DRONE
EL MÁS VENDIDO DEL MUNDO

Fabricante: Parrot.
Autonomía: Hasta 12 minutos.
Peso: 420 g.
Velocidad: 20 km/h.
Tamaño: 52,5 x 51,5 cm.
Precio: 302 euros.
Uso: Es el más vendido de su tamaño y se controla a través del móvil -iPhone o Android-. Incluye una función para que puedas 'emular' batallas con otros AR Drone: en la pantalla de tu teléfono verás como si lanzara rayos láser mientras lucha contra otros aparatos.
+ info: ardrone2.parrot.com

2 PHANTOM 3
PARA SUBIR FOTOS INCREÍBLES CON TU MÓVIL

Fabricante: DJI.
Autonomía: 23 minutos.
Peso: 1,3 kg.
Velocidad: 57,6 km/h.
Tamaño: 59 cm de diagonal.
Precio: 1.200 euros.
Uso: Lleva una cámara incorporada y DJI ofrece una aplicación móvil para subir, directamente, los vídeos e imágenes que toma a YouTube, Facebook, Instagram...
+ info: dji.com/Phantom-3

3 X5C
PARA VOLAR EN CASA

Fabricante: Syma.
Autonomía: 7 minutos.
Peso: 1,3 kilos.
Velocidad: No figura.
Tamaño: 31 cm de largo x 31 de ancho x 8 de alto.
Precio: 60 euros.
Uso: Su manejo es sencillo y está especialmente recomendado para principiantes. Tiene una buena estabilidad y, gracias a su pequeño tamaño, puede manejarse, incluso, dentro de casa.
+ info: amazon.es/x5c+syma

4 BEBOP DRONE 2
HACE FOTOS PANORÁMICAS

Fabricante: Parrot.
Autonomía: 50 minutos en total -gracias a sus dos baterías-.
Peso: 420 gramos.
Velocidad: 50 km/h.
Tamaño: 28 cm de largo x 32 de ancho x 3,6 de alto sin carcasa; 33 x 38 x 3,6 cm con carcasa.
Precio: 700 euros aprox.
Uso: Creado para grabar vídeos y tomar imágenes panorámicas con calidad de 14 Mpx.
+ info: parrot.com/es/productos/bebop-drone



5 SOLO 3DR

TRANSMITE VIDEO EN ALTA DEFINICIÓN

Fabricante: 3DRobotics.
Autonomía: 25 minutos -20 con la cámara-.
PESO: 1.500 gramos.
Velocidad: 88,5 km/h.
Tamaño: 25 cm de alto y 46 cm 'de lado'.
Precio: 1.300 euros aprox.
Uso: Puede transmitir vídeo en alta resolución desde su cámara GoPro a un smartphone o tableta, gracias a su WiFi, con un alcance de 800 metros.
+ info: 3drobotics.com/solo-drone

6 NANODRONE VCAM

HACE MANIOBRAS ACROBÁTICAS

Fabricante: Nanodrone.
Autonomía: Hasta 7 minutos.
Tamaño: 8 cm de largo x 8 de ancho -13 x 13 cm con la carcasa-.
Precio: 144 euros.
Uso: Para principiantes. Graba imágenes en alta calidad mientras realiza maniobras acrobáticas.
+ info: juguetronica.com/drones/nanodrone-vcam.html

7 Q500 +

FOTOS EN FULL HD CON GRAN ANGULAR

Fabricante: Yuneec.
Autonomía: 25 minutos.
Carga: 185 gramos.
Velocidad: No figura.
Tamaño: 42 cm de ancho x 42 de largo x 24 de alto.
Precio: 1.099 euros.
Uso: Transmite vídeo y puede realizar fotografías con resolución Full HD 1080p, o con gran angular -es decir, abarcando un campo de visión de hasta 130º-.
+ info: yuneec.com/products/AerialUAV/typhoon-q500-plus.html

8 VOYAGER 3

GRABA PANORÁMICAS A 360º

Fabricante: Walkera
Autonomía: De 20 a 25 minutos.
CARGA: 320 gramos.
Velocidad: 79,2 km/h.
Tamaño: 47,3 cm de largo x 46,3 de ancho x 30 de alto.
Precio: Desde 2.200 euros.
Uso: Puede grabar panorámicas de 360º y en 3D, gracias a que el soporte donde lleva la cámara puede rotar.
+ info: walkera.com/en/category.php?id=143&parent_id=117

*Los precios son aproximados, y sin carácter contractual.



En Internet ya existe un virus informático que infecta drones

PELIGRO AMAZON

¿Te imaginas recibir 'por los aires' tu última compra en Internet? Eso es lo que pretende el gigante del comercio electrónico Amazon, para lo cual utilizaría drones de reparto que pudiesen transportar objetos de pequeño tamaño. ¿Habrán tenido en cuenta qué pasaría si un ciberdelincuente decide secuestrar el drone que lleva a casa tu nuevo iPhone o tablet de última generación?

Consulta aquí la legislación sobre drones en España.

HACKEAR DRONE

¿PUEDEN LOS HACKERS ROBARTE TU DRONE?

Usarlo para espiar a los vecinos mientras toman el sol en la azotea de su casa, 'estrellarlo' contra algo o alguien o, incluso llegar a 'secuestrarlo'. Como todo aparato tecnológico y conectado, un drone también pueden ser hackeado y puesto 'al servicio del mal'. Un riesgo que es real, tanto con modelos civiles como militares. ¿Cuál es su punto débil? ¿Se puede evitar? **Texto // Elisa Coello**

Cuál es la parte más compleja de un drone? Es el mecanismo de control remoto, que permite desde que un aparato sencillo realice piruetas en el jardín de nuestra casa... hasta controlar drones militares a cientos de kilómetros para atacar a un grupo terrorista. Y esa es, precisamente, su gran debilidad: que entre el drone y la estación de control haya miles de kilómetros de distancia; una distancia que se suple gracias a satélites que hacen de repetidor entre ambos. Los ciberdelincuentes saben que, cuantos más elementos tiene un sistema, más fácil es encontrar sus vulnerabilidades.

En 2011, el ejército iraní secuestró un drone del Pentágono para copiar su tecnología

SECUESTROS DE DRONES, ¿UNA MODA?

Por supuesto, cualquier drone de aficionado podría ser objeto del deseo ajeno -sobre todo si lleva acoplada una cámara de alta resolución tipo GoPro, que vale unos 400€ en cualquier tienda especializada-: basta con que un ciberdelincuente tome su control para que veamos cómo nuestro aparato deja de obedecer nuestras órdenes... y desaparece volando. Así lo demostró el investigador experto en seguridad informática, Rahul Sasi, cuando presentó su 'malware' para piratear drones, el 'Maldrone'. Según explicó, una vez que el drone está infectado, el atacante puede manejarlo o cortarle la energía cuando quiera.

LOS RIESGOS PARA UN CIUDADANO

Pero los peligros pueden ir más allá de un simple robo. Desde hace pocos años, los drones han pasado a realizar tareas cotidianas y han demostrado ser de gran ayuda en trabajos hasta entonces poco accesibles o incluso peligrosos. Así, los drones están funcionando con éxito en la agricultura para fumigar los campos o para labores de vigilancia, pero... ¿y si un hacker maligno los 'manipulase' y esos mismos drones esparcieran pesticidas en dosis letales para las personas o se dedicaran a espiar y grabar a la gente?

LOS ENEMIGOS DEL PENTÁGONO

La situación se torna más seria cuando estos aparatos son militares y están armados para atacar un objetivo. Es el caso de los modelos de EE.UU. Predator y Reaper cuyo sistema de control sufrió un ciberataque a mediados de la pasada década y sus sistemas de control fueron infectados desde tierra. ¿Cuál fue su 'talón de Aquiles'? Su control estaba basado en el sistema operativo Windows de Microsoft... y carecía de antivirus. Una información que no pasó inadvertida al bando enemigo.

La investigación del ciberataque dio a conocer que, a pesar de ser aparatos militares, carecían de comunicaciones cifradas en el sistema de vídeo que transmite las imágenes desde el drone hasta el puesto de control. En 2009, el ejército estadounidense descubrió que su sistema de transmisión de vídeo había sido interceptado por la insurgencia iraquí, que controlaba todo lo que los drones veían y enviaban a las bases a miles de kilómetros. ¿Lo consiguieron con un ataque de ingeniería avanzada? Nada de eso; sólo necesitaron un programa que cuesta... ¡20 euros! ¿La conclusión? Pues que de nada sirve tener un drone casi indestructible y una estación de tierra inexpugnable a ciberataques si se descuida el sistema de comunicación entre ambos.

De esta vulnerabilidad se sirvió Irán para hacerse con un drone estadounidense en 2011. El aparato no tuvo que ser derribado ni sufrió daños en su software si no que, como la propia administración norteamericana reconoció después, un ciberataque interfirió en la señal GPS que guiaba al drone. El ejército iraní consiguió que el aparato aceptara sus órdenes como propias y aterrizó en suelo iraní sin apenas daños.

GAFAS PARA HACER LO QUE NUNCA TE ATREVISTE

Pilotar una nave espacial, enfrentarte al ataque de un tiburón, reparar un gigantesco avión, ver edificios antes de que se construyan o, incluso, asistir en primera fila a conciertos que se celebran a miles de km. ¿Súper poderes? No, son sólo algunas de las aplicaciones de las gafas de realidad virtual, que prometen revolucionar tanto en el mundo del ocio como del trabajo //

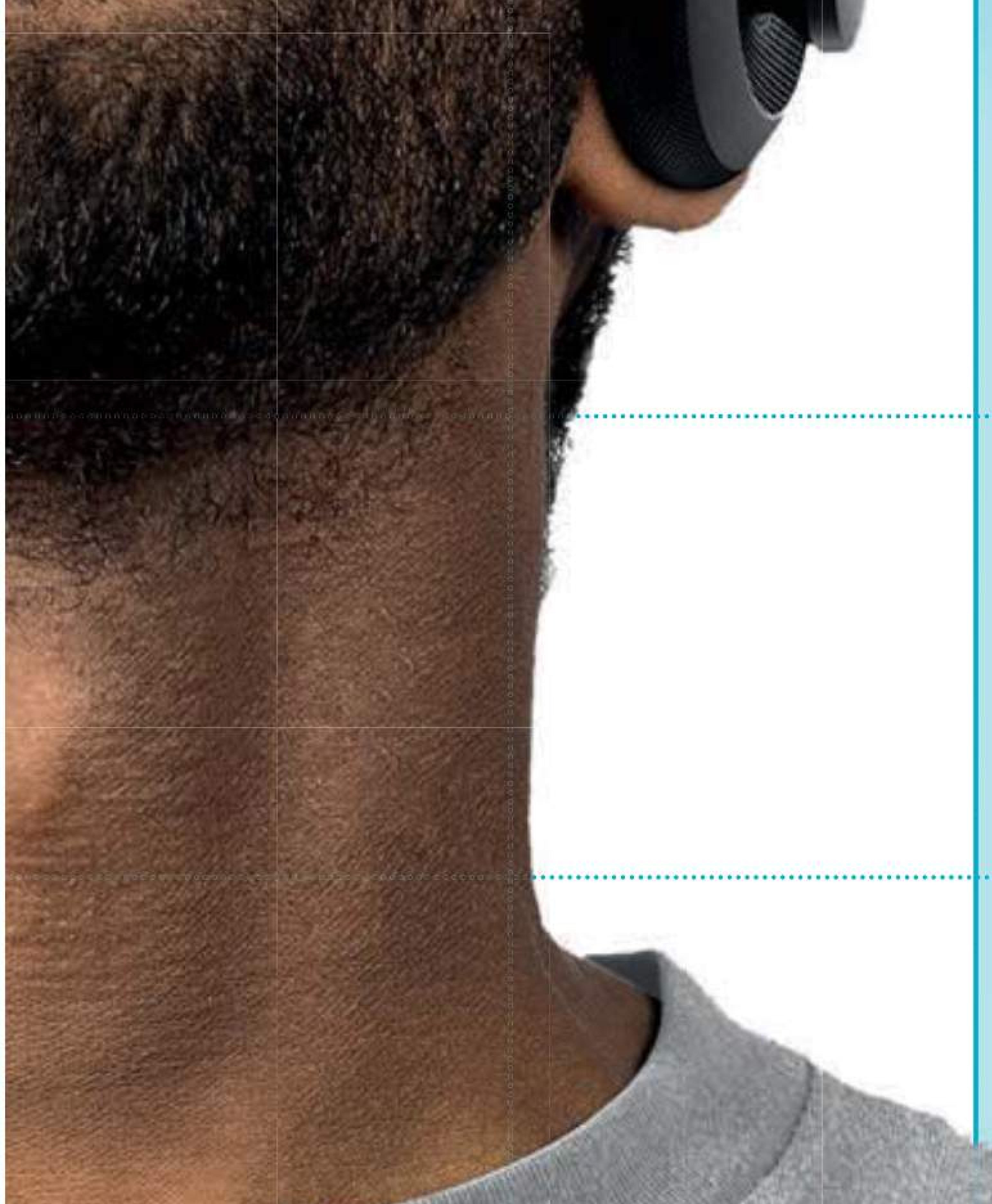
Texto: Teresa Brito



LAS QUE TODOS QUIEREN IMITAR

01 OCULUS RIFT

Oculus VR comenzó como una pequeña start-up -empresa de reciente creación con un futuro prometedor- que Facebook adquirió en 2014 por 2.000 millones de euros. Fueron los pioneros en fabricar gafas de realidad virtual. Su modelo ya está siendo usado por algunas fuerzas armadas para el entrenamiento de sus unidades -tienen acuerdos con DARPA o Samsung-. También tendrán aplicaciones al mundo de la medicina, la industria, el ocio... En 2016 se comercializará la 3ª generación de este modelo pensado para ver películas, jugar a videojuegos o, por ejemplo, conocer paso a paso cómo montar un mueble o reparar un coche... **Precio:** 1.400 euros -no oficial-. **Pantalla:** Una para cada ojo, de 1.080 x 1.200 de resolución. **Lo mejor:** Son la referencia del mercado. **A la venta...** El primer trimestre de 2016. **www.oculus.com**



Qué podrás hacer con las gafas de realidad virtual



Estar 'dentro' de la tele o asistir a conciertos

Podrás ver películas, series o conciertos... como si estuvieras dentro de la pantalla de TV o del cine. Por ahora, apenas hay 'demos' -pruebas-, pero los avances se suceden con rapidez. Por ejemplo, el cantante Paul McCartney ha lanzado una app -gratuita, para Android- con la que puedes ver una actuación con su famoso tema Live and Let Die... desde el escenario, en 360º y con sonido en 3D. Sólo necesitas unas Google Cardboard -unas gafas de bajo coste, que puedes montar tú mismo por 15€ y un smartphone con pantalla de 5 ó 6" de tamaño.

Ir de turismo

El pasado diciembre, la cadena turística Destination BC lanzó, a través de Google Play para Oculus Rift, 'The Wild Within VR Experience': una experiencia virtual para conocer la Columbia Británica -Canadá- y que te permite realizar paseos en barco, rutas por la montaña... sin moverte de casa. Mientras, la hotelera Marriot ofreció a sus clientes la posibilidad de probar unas cabinas que les 'teletransportaban' a Hawai utilizando unas gafas de realidad virtual y simulando también la temperatura de aquel país, el olor de la playa e, incluso, la brisa.

Curar fobias

Los profesionales de la salud y la psicología están comenzando a utilizar esta tecnología en aquellas personas que padecen fobias -por ejemplo, miedo a los espacios abiertos o cerrados, a hablar en público, a subir a un avión-, que les impiden realizar una vida normal. Con estas gafas, consiguen exponer a sus pacientes, poco a poco, a situaciones controladas, para que superen sus miedos.

Sacar mejores notas

Las gafas de realidad virtual permitirán a los estudiantes simular situaciones reales que les ayuden a aprender más rápido. Por ejemplo, los de medicina serán capaces de realizar operaciones virtuales; los de mecánica, sabrán reparar los componentes de un avión; los de biología descubrir cómo es una planta por dentro... Incluso los estudiantes más jóvenes las podrán usar para viajar a distintos lugares y épocas para aprender geografía o historia. Según diferentes estudios, estas tecnologías aumentarán la motivación de los alumnos en más de un 90% y mejorarán las notas en más del 30% de los casos.

Elegir tu coche y aprender a conducir seguro

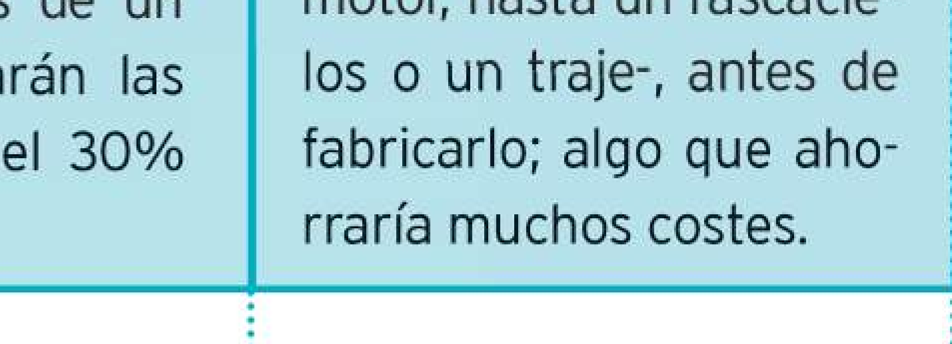
Toyota ha lanzado el programa TeenDrive365 para prevenir a adolescentes y a sus padres sobre los peligros de distraerse al volante. Con las gafas de realidad virtual, exponen al conductor a situaciones que podrían distraerle, como una llamada mientras está al volante. Por su parte, Ford ya las utilizan para que sus clientes puedan ver los interiores y exteriores de sus vehículos en alta definición en el concesionario, cuando el coche deseado no está físicamente en las instalaciones.

Meterse dentro de los videojuegos...

Es uno de los grandes sueños de los aficionados a los videojuegos: utilizar la realidad virtual para 'introducirse' en el juego y recorrer, en primera persona, los más originales mundos imaginarios o enfrentarse con los villanos más conocidos de las consolas.

Diseñar edificios, vehículos, moda...

Estas nuevas herramientas permiten ver, en realidad virtual y en tres dimensiones, cómo quedaría cualquier diseño -desde la pieza de un motor, hasta un rascacielos o un traje-, antes de fabricarlo; algo que ahorraría muchos costes.



Estas son las que pronto podrás comprar

IDEALES PARA JUGAR...

02 MORPHEUS

Son las gafas de Sony para su consola PlayStation4. Con un diseño futurista y ergonómico, te permitirán pilotar una nave espacial -con el juego Eve Valkyrie-, convertirte en un robot y luchar contra un monstruo -con Monster Escape- o resistir al ataque de un tiburón -con Deep Blue-. Además, cuenta con sonido 'envolvente' y unos sensores para que la consola sepa en todo momento dónde estás. **Precio:** No definido. **Pantalla:** 5,7" y 1.920x1.080 de resolución. **Lo mejor:** Está diseñado para que se ajuste a tu cabeza, pero sin ejercer presión sobre ella. **A la venta...** Se calcula que a mediados de 2016. **playstation.com**





LAS MÁS INTERACTIVAS

03 HTC VIVE

Cuentan con más de 70 sensores, posicionamiento láser, dos cámaras que monitorizan tus movimientos, acelerómetro, giroscopio, etc., para que puedas desplazarte por una superficie de hasta 25 m2 mientras simulas que estás en el espacio, viajas por la antigua Roma, sujetas objetos virtuales -utilizando otro mando específico-... De momento, su uso se centrará en el mundo de los videojuegos, pero ya se está trabajando con el canal HBO para ofrecer contenidos específicos. **Precio:** No definido. **Pantalla:** una por ojo, con 1.080x1.200 de resolución. **Lo mejor:** Sus dos pantallas consiguen que la experiencia sea más real. **A la venta...** a finales de 2015. **htcvr.com/es**

LAS MÁS POLIVALENTES

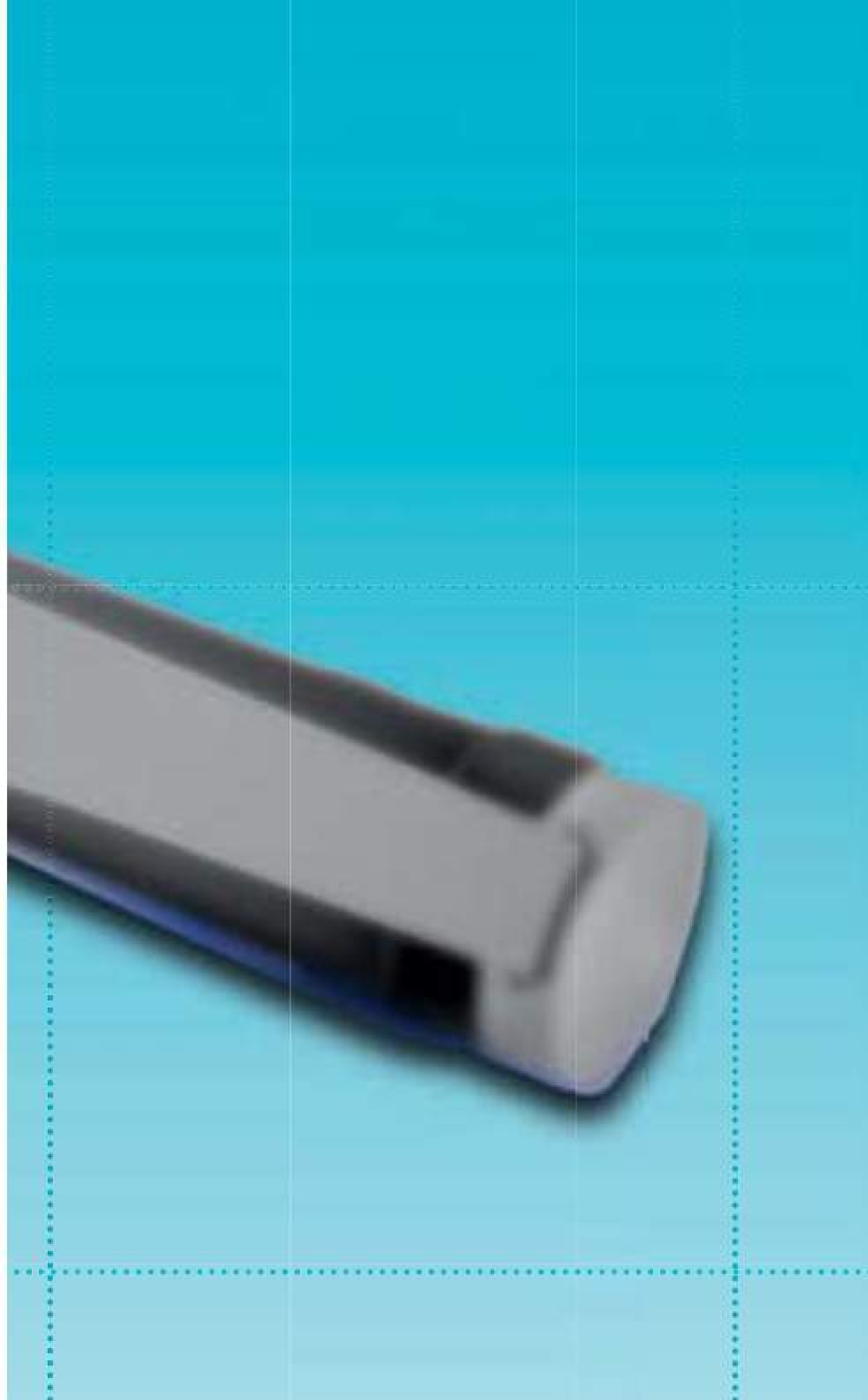
04 AVEGANT GLYPH

Pueden conectarse a cualquier dispositivo -smartphones, tablets, ordenadores, consolas de juegos, televisión...- a través de un USB. Utilizan una tecnología diferente al resto de gafas: se llama 'Virtual Retina Display' y es un sistema que, mediante una lámpara led de baja potencia y el uso de dos millones de microscópicos espejos, reflejan imágenes que se proyectan directamente en tu retina. **Precio:** 540 euros. **Pantalla:** No tiene. **Lo mejor:** Todo lo que ves en tus dispositivos te parecerá mucho más realista. **A la venta...** este otoño. **avegant.com**/

LAS MÁS ORIGINALES

05 MICROSOFT HOLOLENS

A diferencia de otros modelos, estas gafas no sirven para 'adentrarse' en mundos virtuales, sino para alterar lo que ves con hologramas en 3D. Así, puedes ver la televisión en una pared en blanco, 'caminar' por otros planetas... Además, resulta especialmente útil para que diseñadores, ingenieros o arquitectos vean sus proyectos antes de construirlos. **Precio:** Se calcula que entre unos 800 y 1.000 euros. **Pantalla:** Es transparente, para que veas la luz e imágenes -en alta definición- que proyectan. **Lo mejor:** Es inalámbrico y no necesita mandos -funciona con gestos-. **A la venta...** Aún por definir. microsoft.com/ **microsoft-hololens**





PARA CREAR TU PROPIO VIDEOJUEGO

06 OSVR RAZER

Estas gafas están pensadas únicamente para videojuegos. Son 'de fuente abierta': eso significa que cualquiera con conocimientos de programación puede descargar sus archivos y crear su propio juego para ellas.
Precio: No disponible. **Pantalla**: 5,5" y 1.920x1.080 de resolución. **Lo mejor:** Ya cuenta con el apoyo de 24 compañías de videojuegos. **A la venta...** A principios de 2016. No obstante, ya está disponible -por unos 270 euros- el Hacker Dev Kit, un prototipo avanzado para que los desarrolladores puedan comenzar a crear sus juegos de cara al lanzamiento de la versión definitiva.razerzone.com/osvr

Cuáles puedes usar ya con tu smartphone

Las gafas de realidad virtual llevan años de desarrollo... y su evolución no ha estado exenta de problemas. Las imágenes que ofrecían los primeros prototipos estaban lejos de parecerse a la 'realidad' y algunos modelos producían mareos a los usuarios. Solucionados estos inconvenientes, el principal escollo que quedaba por salvar es el desarrollo de un software -el programa que las hace funcionar- que no fuera excesivamente caro, de forma que se consiguiesen productos de calidad pero que, por precio, no fueran inaccesibles para el gran público. ¿Cuál es la solución? Aprovechar el software de tu teléfono y acoplar éste a una estructura -más o menos avanzada-, dotada de unas lentes que permitan ver en 3D o en realidad aumentada.

LAS QUE MÁS SE POPULARIZARÁN



07 SAMSUNG GEAR VR

Solo para Samsung, son fáciles de usar y emplean la tecnología de las Oculus Rift. Contarás con visión panorámica en 360º e incluye acelerómetro, giroscopio, sensor de proximidad... para que tus movimientos y los de las imágenes que ves estén perfectamente sincronizados. **Precio:** 200 euros. samsung.com

EL PRECIO MÁS ASEQUIBLE

08 ARCHOS GEARVR

Consta de una estructura sobre la que se acopla cualquier smartphone -con pantalla de entre 5 y 6"-, y en el que tienes que instalar la aplicación gratuita Archos Video Player. Con ella, puedes reproducir películas en 2D -pero con ángulos mayores, como si estuvieras en el cine-, y también en 3D. **Precio:** Unos 25 euros. **archos.com**

EL DISEÑO MÁS ELABORADO

09 ZEISS VR ONE

Gracias a sus lentes de precisión incorporadas, a este sistema se le puede acoplar cualquier móvil con pantalla de entre 4,7 y 5,2" de tamaño -más adelante llegarán nuevos 'adaptadores' para otros teléfonos- para ver películas y jugar en formato 3D panorámico y disfrutar de la realidad aumentada -consiste en ver imágenes superpuestas sobre las cosas que te rodean-. **Precio:** 129€. **zeiss.com**

LA IMAGEN DE MAYOR TAMAÑO

10 LAKENTO MVR

Se trata de una montura de gafas de realidad virtual, con unas lentes de 42 mm, en las que se puede acoplar un teléfono móvil -de entre 4 y 6,4" de tamaño-. Con ellas -y previa descarga de una app- puedes ver cualquier contenido de tu móvil -fotos, videos, juegos...-, pero como si estuvieras delante de un televisor de 300" y en 3D. Además, el pack incluye dos juegos: Sharks VR -sobre tiburones- y House of Terror VR -la casa del terror-. **Precio:** 59 euros. **lakento.com**

Así las utilizan los Ejércitos...

- Noruega ha sido el primer país en utilizar esta tecnología en sus simuladores de combate -concretamente para los tripulantes de sus carros de combate-.
- En España, el Ejército del Aire utiliza un simulador de realidad virtual para entrenar a sus paracaidistas. Además, la multinacional española ITP está desarrollando esta tecnología para el mantenimiento de algunas partes de los cazas F18.
- EE.UU. y el Reino Unido están experimentando con estos nuevos dispositivos, para realizar ejercicios de simulación y reconocer terrenos hostiles de forma virtual.
- También pueden utilizarse para prácticas de tiro, como es el caso de Virtual Gun 3D, un simulador español táctico de infantería pensado para entrenamientos militares y policiales.
- La DARPA -Agencia de Investigación de Proyectos Avanzados del Pentágono- está llevando a cabo el Plan X. En él contempla usar gafas de realidad virtual para que sus cibercomandos visualicen todo tipo de datos cuando repelan un ataque.

PARA FANS DE OTRA GALAXIA

STAR WARS

Desde el 18 de diciembre se proyecta en los cines la última y esperada entrega de Star Wars. Es la primera bajo la supervisión de Disney, por lo que todo el mundo tiene sus ojos puestos en ella. Si eres un verdadero fanático de la Fuerza, atento a los gadgets que te permitirán vivir la nueva aventura espacial en casa, el coche y en cualquier viaje que hagas.



PORTÁTIL HP DEL LADO OSCURO DE LA FUERZA

Edición limitada de HP inspirada en 'el lado oscuro', con pantalla Full HD de 15,6", un procesador Intel Core i6, memoria RAM de 8GBs y tarjeta gráfica NVIDIA GeForce 940M, de 2GB, para dedicarlo a videojuegos.

800€
store.hp.com



CARGADOR DE MÓVIL PARA EL COCHE R2-D2

Este robot mantendrá todos tus dispositivos móviles cargados y listos para cualquier misión. Está pensado para que lo instales en el sujetavasos de tu vehículo, y cuenta con dos tomas USB para poder conectar dos dispositivos al mismo tiempo.

29,70€
www.thinkgeek.com



CASCOS DE EDICIÓN LIMITADA STAR WARS

Estos cascos, disponibles en cuatro modelos diferentes -Boba Fett, Stormtrooper, Alianza Rebelde e Imperio Galáctico-, ofrecen un aislamiento acústico perfecto, una calidad de sonido excelente y, además, son plegables para que que sea fácil llevarlos siempre encima.

139€
www.thinkgeek.com



EL TROLLEY PREFERIDO DE DARTH VADER

Está inspirado en el atuendo de Darth Vader y sus medidas son aptas para llevar como equipaje de mano en la cabina del avión. Fabricado al 100% en aluminio, sus cuatro ruedas pueden girar 360º -lo hace más manejable-. Además, cuenta con un asa extensible y varios compartimentos interiores, que te permitirán organizar con precisión todo lo que necesites en tus viajes.

59,37€ / www.thinkgeek.com



VIVE LA FUERZA DE STAR WARS CON BATTLEFRONT

Una de las grandes novedades del nuevo año es la nueva versión del conocido Battlefront, que te permitirá sumergirte en el universo Star Wars con batallas increíbles, gráficos muy cuidados y todo tipo de detalles. Será uno de los videojuegos bélicos más vendidos del 2016 para PS4.

59€
www.ea.com/StarWarsBattlefront

REGALA UNA MASCOTA POR REYES

Pueden hablar contigo, seguirte, hacerte compañía o limpiar tu casa. Si quieres disfrutar del 'futuro', aquí tienes los mejores humanoides para ti... o tus hijos. Texto // Santiago Lauja

Los robots son la élite del mundo de la informática: ordenadores que pueden interactuar verbal o físicamente con las personas y en todo tipo de tareas -limpiar, enseñar, cuidar enfermos-", explica el mayor coleccionista de Europa, Pablo Medrano, con cerca de 300 piezas -se pueden ver en el Museo del Robot, en Madrid, (www.therobotmuseum.eu)-. "Muchos están desarrollados con tecnología militar y forman parte de la nueva oleada tecnológica que estamos viviendo". Por eso, recomienda introducir, desde ya, a los niños -y a los mayores- en este mundo. "Con conocimientos básicos de programación y sólo 300€ puedes 'jugar' con modelos muy completos. El punto de partida es tener claro tu presupuesto y el uso del robot", añade Daniel Bayón, de la tienda de robots Juguetrónica. Los hay incluso basados en películas como el simpático Sphero BB-8 'réplica' del utilizado en Star Wars 'El despertar de la fuerza'.



POPPY PROJECT

Quiere ser como tú

85 cm • 3,5 kg • 8.880€ • www.poppy-project.org

Se trata del primer robot humanoide fabricado con piezas elaboradas a partir de una impresora 3D y ha sido diseñado por científicos franceses, con fondos de la UE. Cuenta con un software 'de programación abierta' -o sea, todo el mundo puede utilizarlo- que permite programarlo para cualquier tarea y, gracias a sus sistemas de comunicaciones, puede interactuar con teléfonos móviles.



0

PEPPER

Aprenderá… si le enseñas

120 cm • 28 kg • no se vende: se alquila • www.aldebaran.com

Es el primer robot ‘emocional’ que ha sido diseñado para ser una compañía del ser humano en su vida diaria; de hecho, es capaz de comunicarse contigo, tiene cierta personalidad y puede mostrar sentimientos –con gestos, el color de sus ojos con ciertas palabras-. No se maneja con ningún mando, ratón u ordenador: basta con hablarle, tocarle o aproximarte para que reaccione. Su batería dura 12 horas y cuando se va a agotar, Pepper se desplaza solo a su punto de recarga.

2

HEXBUG ARAÑA XL

Tiene tres velocidades

40 cm • 458 grs • 40€ • www.juguetronica.com

Se trata de una araña radiocontrol con tres velocidades hacia delante y una hacia atrás. Es capaz de girar 360º, incluida su cabeza. Tiene seis patas y es un 65% más grande que Hexbug araña. Con el mando se pueden controlar dos arañas a la vez y hacerlos pelear entre sí. Se puede elegir entre el modelo en rojo o en azul.



3

NAO

Para empezar en serio

58 cm • 4,3 kg • 6.000€ • Robotslab.com

Hasta 2014, sólo se vendía a universidades para proyectos de investigación... pero ahora se comercializa al gran público a la mitad de precio -de casi 12.000 que costaba, a 6.000 euros-. Puede andar, subir escaleras y responder a cualquier orden hablada. Es el mejor modelo para comenzar a programar y centenares de ingenieros ya han desarrollado programas para él -más info. en robotslab.com-.

4

LEGO MINDSTORMS

Para niños mayores

50,2 cm • 1,8 kg • 349€ • www.juguetronica.com

Está hecho con piezas de Lego -hay hasta 550 distintas- sobre las que se acopla un pequeño cerebro informático que se puede programar para que el robot realice todo tipo de tareas -caminar, hablar, moverse... -. Se puede controlar con un mando a distancia o el móvil e incluye instrucciones muy detalladas. Es el mejor robot para que los niños, desde 10 años, aprendan a programar.

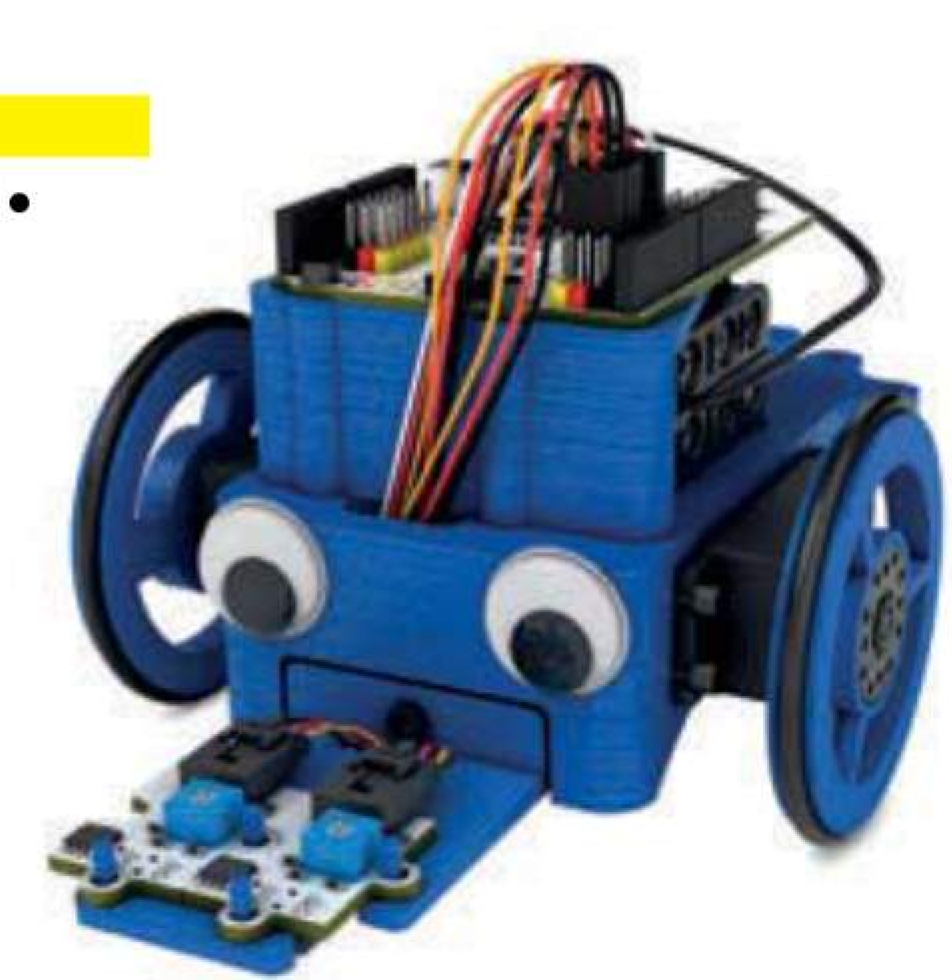
*Los precios son aproximados, y sin carácter contractual.

5

BQ PRINTBOT

Para niños 'digitales'

64 cm • 3,5 kg • 19,9€ • www.bqreaders.com



Disponible en verde, morado, rojo, azul y amarillo, el PrintBot Renacuajo es un juguete compuesto de dos docenas de piezas plásticas y electrónicas que te permitirán ensamblar tu primer minirobot de forma fácil y divertida. La empresa que lo ha creado, la española BQ, también vende una impresora 3D -por 1.700€- para que puedas crearte piezas de otros tamaños y formas e ir completando el modelo original.

6

ROBOSAPIEN X

Con 'tecnología' de la NASA

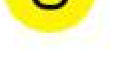
35,5 cm • 2 kg • 99€ www.mastrum.com





Es el robot humanoide más barato y completo del mercado. Se puede manejar a través de móviles iOS/Android -o bien mediante su propio mando a distancia- y ha sido diseñado por Mark Tilden -un ex-ingeniero de la NASA que trabajó en el Robot de exploración de Marte-. Tiene 67 funciones pre-programadas -se le pueden añadir 84 más- entre las que destacan las de andar, bailar, coger pequeños objetos -bolis, revistas, etc.-.





7

PLEO V2 RB

Muestra sus emociones

20 cm • 1,5 kg • 399€ • www.juguetronica.com

Este dinosaurio parece real, no solo por su capacidad para mostrar emociones, sino también por sus conseguidos movimientos y su evolución -desde cría hasta adulto-. Según cómo le trates, tu PLEO V2 RB será tímido, obediente, 'cabezota', etc. Su estado de ánimo te indicará qué necesita. Por ejemplo, si gime es que algo le da miedo, quizás porque le hayas agarrado muy fuerte.

8

PARO

Mascota casi de verdad

50 cm • 5 kg • 4.000€ • www.parorobots.com

Con la forma de una cría de foca y del tamaño de un bebé, este simpático robot -que se lanzó en 2003 y ya va por su octava generación- está siendo utilizado para hacer compañía a personas mayores, sobre todo las que padecen Alzheimer, ya que interactúa con ellas reaccionando al tacto -se deja acariciar y rascar- y a la voz. Ha sido creada para generar afecto con sus propietarios.



9

PERRO ROBOT ZOOMER 2.0

Edúcale para que obedezca

20 cm • 450 g • 99€ • http://www.bestofrobots.es/

Si lo adiestras bien, te reconocerá, te responderá y se comportará como tú quieres. Le puedes enseñar a que te dé la pata, que dé un paseo junto a ti o que haga de zombi. Al actuar como una mascota de verdad y necesitar efecto y atención, servirá de aprendizaje a los más pequeños por si algún día quieren tener un perro. A través de sus ojos y de sus acciones, sabrás si es feliz.

¿SE PUEDE HACKEAR UN ROBOT?

YA HA HABIDO VIRUS INFORMÁTICOS PARA DRONES... ¿POR QUÉ NO PARA ROBOTS?



Deepak Daswani

EXPERTO DE DELOITTE CYBERSOC ACADEMY

Te prepararán el café, conducirán por ti e, incluso, te operarán. Pero, imagina que un criminal se hace con el control de tus robots y le ordena que no te sirva el desayuno, se salten los semáforos o... te maten. El que ha sido hasta hace pocos meses responsable de contenidos e investigación en ciberseguridad del Insituto Nacional de Ciberseguridad -INCIBE-, nos cuenta hasta qué punto es posible, también en el ámbito militar.

¿Qué está pasando con los actuales drones¿¿Se puede interferir?

El uso de drones -vehículos aéreos no tripulados, UAV- se ha incrementado tanto en el ámbito civil como militar y, además de su utilidad, también han evidenciado algunos problemas de seguridad con incidentes importantes. Entre los más conocidos destaca la interferencia del canal de vídeo de un drone del ejército estadounidense, en 2009, por parte del ejército iraquí. Y lo más alarmante: lo consiguieron usando software al alcance de cualquiera – el SkyGrabber que se utiliza habitualmente para interceptar canales de música, televisión y vídeo por satélite-. ¿Por qué? Pues, porque, en ese momento, muchos de los aparatos no tenían sus transmisiones cifradas. En 2011, tuvimos otro incidente relacionado con la flota de vehículos aéreos no tripulados del ejército de Estados Unidos. Un keylogger -un software que monitoriza y registra todas las pulsaciones del teclado de un ordenador- infectó los sistemas de la flota de drones de la base aérea de Creech. Teniendo en cuenta que estos drones se usaban en misiones de combate y reconocimiento, podemos deducir la importancia de esta infección. Curiosamente, sus ordenadores no estaban conectados a Internet… por lo que fueron infectados a través de discos duros externos que alguien conectó. Por fortuna, según fuentes del ejército americano, el incidente no puso en peligro ninguna misión ni vidas humanas.

La clave para hacer robot seguros...

En el mundo de la seguridad nunca hablamos de sistemas 100% seguros, sino de sistemas 'confiables'. No se puede establecer un 'decálogo mágico' que permita garantizar la absoluta seguridad y esto es válido tanto para drones, como para robots, smartphones, ordenadores, neveras, hornos, o cualquier tipo de dispositivo inteligente. Eso sí, evidentemente, se han de seguir una serie de principios, directrices y buenas prácticas en el ciclo de desarrollo de los productos que nos permitan maximizar la seguridad de los mismos. Estos pasan por intentar aplicar los principios de defensa en profundidad, establecer políticas de seguridad para el uso de los dispositivos, fortificar los sistemas de autenticación a los mismos, garantizar la seguridad de las comunicaciones con esquemas robustos de cifrado, realizar auditorías del código fuente así como tets de penetración buscando posibles vulnerabilidades que puedan ser explotadas,…

Qué sería capaz de hacer un hacker con un robot...

Esta pregunta es muy genérica, pero yo diría que lo que podría hacer un hacker con un robot es….hackearlo!-risas-. El mayor peligro es que un ciberdelincuente, no un hacker -los hackers somos los buenos-, tome su control y saque provecho de sus acciones. Pero no es sencillo: para comprometer un sistema éste ha de tener un fallo que pueda ser explotado. Evidentemente, dependiendo del ámbito en concreto, y la criticidad del dispositivo, se está trabajando desde la industria en incorporar medidas de seguridad que permitan garantizar el correcto funcionamiento de estos dispositivos con el fin de evitar que atacantes malintencionados puedan hacerse con el control de los mismos.

> “Viendo el nivel de sofisticación de los ataques, si un criminal se plantea hacernos daños... lo hará”

Qué te da miedo de los robots...
El mayor peligro es que un atacante pueda tomar el control y lo utilice en su favor o bien evite que pueda cumplir adecuadamente su función. Si esa función es crítica, y el robot presenta vulnerabilidades que pueden ser explotadas, el impacto contra vidas humanas, infraestructuras, instalaciones u organizaciones sería inimaginable.
Como hacker te preocupa...
¡Quedarme sin Internet! La verdad que hace unos años podríamos haber dicho muchas cosas pero a día de hoy, vivimos en un escenario en el que la realidad supera a la ficción. Viendo el nivel de sofisticación de las amenazas, los ataques tan dirigidos donde organizaciones cibercriminales roban información de manera silenciosa durante muchísimos años, los casos de ciberespionaje entre agencias gubernamentales de diferentes naciones, escándalos como PRISM o la operación Tempora, vulnerabilidades como HeartBleed o Shellshock que llevan presentes durante tanto tiempo, o misteriosas vulnerabilidades, como el Goto Fail de Apple, uno se plantea que, si realmente alguien quiere tener acceso a nuestra información y con ello a nuestra vida, al final, lo tendrá.

CHEMA ALONSO

SE HIZO FAMOSO POR SUS CONOCIMIENTOS EN UNA DE LAS CONFERENCIAS DE HACKERS MÁS POPULARES DEL PLANETA -DEFCOM-, FICHÓ POR MICROSOFT Y AHORA TRABAJA PARA TELEFÓNICA. NADIE MEJOR QUE ÉL PARA SABER LO VULNERABLE QUE ES NUESTRO MUNDO. TEXTO JM.VERA

Bajo su apariencia de persona despreocupada y con su sempiterno gorro bicolor de snowboard se esconde uno de los expertos en ciberseguridad más respetados -y temidos- de España. Hacker mediático, bloguero de éxito y creador de muchas de las herramientas informáticas que nos permiten navegar más seguros en Internet, Chema Alonso vive pegado al teclado de su portátil. Nos ha recibido en su despacho de Eleven Paths, la compañía de Telefónica que él dirige, para contarnos qué se está haciendo bien y mal en el mundo 'virtual', cómo podemos defendernos del 'lado oscuro' de Internet y en qué nuevos y sorprendentes proyectos se encuentra inmerso.

Tu blog se titula 'Un hacker en el lado del mal'; ¿qué historia hay detrás?
Hace años, la gente comenzó a hablar de hackers buenos y malos. En este 'mundillo' se consideraba que Microsoft era 'de los malos'; yo trabajaba allí y al igual que el resto de los empleados éramos vistos como 'los del lado del mal', así que recurriendo a mi sentido de la ironía, decidí hacerme llamar "El Maligno". De hecho, me lo llamaban porque alguien dijo que yo era como el Diablo disfrazado de John Lennon. Y de todo esto, mi blog se llamó "Un hacker en el lado del mal".

Entonces, te ves como un 'hacker del mal' que ahora está al servicio del bien...
La palabra hacker está muy estigmatizada, parece que eres un delincuente. Cuando te presentan como tal siempre tienen que aclarar apresuradamente que eres 'de los buenos'. Pero, para mí, ser hacker es un ideal, algo que todos soñamos alcanzar. Admiro a los hackers... pero no a los ciberdelincuentes. Lo cierto es que cada vez más empresas los contratan: Google ha fichado a Charlie Miller y Facebook o Twitter también cuentan en su nómina con grandes hackers...

¿Cómo te convertiste en uno de ellos?
Comencé en la informática muy joven, con 12 años, haciendo cursos en una academia de mi barrio -La Loma, en Móstoles-, donde decían que era "el trabajo del futuro". Empecé programando en Basic -un tipo de lenguaje informático- con un ordenador Amstrad... pero, hasta que no fui más mayorcito no me di cuenta de que me gustaba esto de la ciberseguridad. Por eso, estudié la carrera técnica de informática, luego me matriculé y aprobé la licenciatura, el master e, incluso, me doctoré. Cuando empecé a trabajar me encantaban las bases de datos y del entorno Oracle -un sistema de gestión de base de datos-. El 25 de diciembre de 1988, me apunté a un 'reto hacking' -un concurso de hackers- y descubrí las técnicas de inyección de código SQL -permiten introducirte en bases de datos aprovechándote de alguna vulnerabilidad informática-. Fue increíble. Respecto a lo que sabía, fue como pasar de cortar



"Estamos en una guerra encubierta a través de móviles, tablets, PC's..."



mantequilla con un cepillo de dientes... a hacerlo con un cuchillo caliente. Y, a partir de ahí, me enamoré del hacking y no he podido parar... hasta crear la empresa 64 Bits Soluciones Informáticas.

Con tanto tiempo entre ordenadores, no serás 'mucho de libros'

Al contrario... ¡me encantan! Cuando era joven leía dos o tres libros por semana. Siempre he sido un poco solitario... y un poco raro: salía a pasear el perro y, al mismo tiempo, leía.

¿Un hacker 'nace' o 'se hace'?

Para ser bueno hay que ser un 'empollón' y, al mismo tiempo, tener una pasión brutal; los mejores son capaces de 'echar horas', meses y años para resolver un misterio. Esto no es ciencia infusa: todos los que destacan leen mucho y estudian todo el día, pero no de la forma académica a la que estamos acostumbrados. Aquí no existe la magia, así que eso de que "soy un genio y las cosas me salen por intuición", pocas veces funciona. Algunos hackers tienen una mente preclara, pero no es mi caso ni el de la mayoría, así que la clave es ser constante, trabajador y disciplinado.

¿Qué diferencia a uno 'bueno' de uno 'malo'?

Técnicamente, el malo es el que no se fija en los detalles, no estudia bien las cosas, es descuidado...

Lo peor que serías capaz de hacer con tus conocimientos

No quiero ni pensarlo -risas-.

¿Te puedes hacer millonario con esto?

Se puede ganar mucho dinero, poco, medio o regular. Hay algunos que 'venden vulnerabilidades' que sólo ellos han encontrado -es decir, descubren fallos en algún sistema o programa y después 'avisan' a las empresas, que les pagan por esa información- y se hacen de oro. En las empresas tecnológicas, esta profesión está cada vez mejor valorada y bien pagada... pero es normal porque, en definitiva, hablamos de investigadores que tienen un nivel alto para realizar auditorías de seguridad y 'pentesting' -de 'penetration test', es una forma de evaluar la seguridad de los equipos y las redes de comunicación simulando un ataque informático-.

¿Reconocerías a un hacker por la calle?

Es difícil, ya que puede ser quien menos te esperas. No te puedes dejar engañar por el aspecto.

¿Te desprenderás de tu gorro algún día?

Me lo estoy pensando. En algunas conferencias digo: "soy Chema... ya me conocéis, así que no hace falta que me ponga el gorro, ¿verdad?". Y la gente me dice, "¡que se lo ponga, que se lo ponga!". Sólo tengo este, así que el día que lo pierda... ¡será un drama! Algunos han llegado a decir que soy como el chef de la película

"LA SEGURIDAD AL 100% NO SE PUEDE GARANTIZAR"



de Disney 'Ratatouille' que llevo una rata bajo el gorro... que es la que sabe hackear. La verdad es que comencé a llevarlo medio en broma: estábamos presentando el sistema operativo Windows Vista y montábamos como un teatrillo, representando que veníamos de hacer snowboard -¡era verdad, habíamos estado en la nieve!-, al tiempo que poníamos las diapositivas. Lo cierto es que a la gente le hizo gracia... y ya me quedé con el gorro... aunque ahora hay veces que da mucho calor -risas-.

¿Y te cortarías el pelo?

Yo he llevado el pelo largo desde joven, aunque me lo corté, por obligación, cuando comencé a trabajar. Sin embargo, llegó un momento en el que me lo volví a dejar largo, como acto de rebeldía: "si no te gusta, no trabajes conmigo", pensaba. ¿Me lo volvería a cortar? Tal vez, si tuviera que ir a algo tan serio como un entierro.

¿Hay una edad para jubilarse en esta profesión?

No: ahí tenemos a Steve Wozniak -uno de los creadores de Apple- que sigue trabajando en esto a sus 64 años.

Qué no se ha dicho del ciberespacio...

La gente debe tener claro que muchos de los rumores que se dicen, aunque parezcan de ciencia ficción... seguramente sean ciertos. Por ejemplo, se ha dicho que la NSA -agencia de inteligencia estadounidense- intercepta todos los emails, que está elaborando una gigantesca base de datos con las caras de la gente... Aunque suene exagerado, podría ser verdad.

¿Se puede 'derribar' un país utilizando Internet?

Es posible... pero no basta con pulsar un botón rojo, como en las películas. A través de Internet hemos conocido en los últimos años vulnerabilidades tan serias y preocupantes que, de haber caído en malas manos, podrían haber provocado una catástrofe.. No hay que ser alarmistas, pero tenemos que estar preocupados y preparados. Por eso, todos los países están poniendo en marcha muchas medidas relacionadas con la ciberseguridad. El otro día en una reunión con cuerpos de seguridad del Estado que trataba sobre el ciberespacio, les dije: "seguro que hay planes de contingencia por si un ejército enemigo invade con sus carros de combate la Gran Vía, pero... ¿los hay también si alguien 'tira abajo' los servidores de la Bolsa de Madrid o inutiliza los semáforos de Barcelona?" Me dijeron que... están en ello.

El sitio web más seguro que conoces...

¡Qué difícil! Basta que diga uno para que alguien 'se pique' y lo ataque -risas-. La seguridad al 100 % no se puede garantizar, porque, de repente, aparece un nuevo virus y se acabó. El más seguro es el que está administrado con más cariño.

¿Y el más vulnerable?

Aquel cuyo administrador piense: "A mí no me van a atacar".

A quién hay que temer en el ciberespacio...

Hay una frase que dice: "Líbrame del agua mansa, que del agua brava me libro yo". Así que… También hay otra máxima que yo repito mucho: "En el mundo sólo hay lobos y corderos... y si no te toca ser lobo, te toca ser cordero", así que hay que elegir muy bien en qué bando quieres estar.

¿Invertimos lo suficiente en ciberseguridad?

Muchos países del mundo dedican ingentes cantidades de dinero a este campo... y no hay duda de que se trata de una inversión más que justificada. Aún así, uno no siempre se encuentra a salvo de todo. ¿Está España preparada para hacer frente a una invasión terrestre? Seguramente, frente a muchos países no y nos 'machacarían'... pero sí se pueden tomar medidas contra los riesgos más peligrosos e inminentes. Ocurre lo mismo con la ciberseguridad. De cualquier forma, siempre podría ocurrir lo que pasaba en la película 'Juegos de Guerra' -que un chico ponga en jaque la seguridad nacional-. Por eso, a diario, la gente que se dedica a esto está atenta a todo lo que sucede en Internet, incluso en sus rincones más profundos. ¿El reto? Saber antes que nadie si alguien, en algún lugar, ha dado con una vulnerabilidad desconocida.

¿Peligra nuestra Seguridad Nacional?

Decir que sí sería alarmar a la gente...

pero decir lo contrario tampoco se ajustaría a la realidad. En cualquier caso, y aunque en este campo se está trabajando y mejorando, siempre hay que hacer más y más. Hay que hacer mejor los procesos internos para ser mejores. La Seguridad Nacional es una preocupación que todos debemos tener y que hay que cuidar y trabajar.

¿Conoces al presidente Rajoy?
Sí, he estado en La Moncloa con el equipo de Rajoy, hablando sobre temas de emprendedores y de tecnología. Como curiosidad, mientras estaba allí coincidió que yo tenía que entrar 'en directo' y por teléfono en el programa de radio de Javi Nieves, en la Cope, así que en La Moncloa me dejaron solo en un despacho para hablar con tranquilidad. Al decirle a Javi donde estaba, empezó a decirme: "venga, aprovecha y métete en el ordenador"... mientras nos escuchaba toda la audiencia.

Algunos dicen que ya estamos en guerra...
Estamos en guerra, pero de forma encubierta, a través de smartphones, con Zero Days -vulnerabilidades que nadie conoce- y con 'exploits' -programas para espiar sistemas informáticos-. El ciberespacio permite realizar operaciones militares cuya autoría es casi imposible de conocer. Sirva como ejemplo el caso del virus Stuxnet que, en 2011, hizo retroceder una década el programa nuclear iraní. Siempre se ha atribuido a EE.UU., pero nadie pudo demostrarlo…

¿Te ves salvando el mundo?
Trabajo mucho con los cuerpos de seguridad del Estado y con cualquier organismo que me lo pide... Si me llamaran para hacer frente a una crisis, seguro que podría montar, al momento, un equipo de 'killers' -entre civiles y militares- para hacerle frente. Lo cierto es que hay gente muy preparada en los ejércitos, la Guardia Civil, etc... que ocupan puestos críticos; el error sería que se les cambiara de destino sólo porque les ascendieran. Si se hace, estamos tirando a la basura un montón de conocimientos y de habilidades.

¿Qué le recomiendas al CNI y a Defensa para que no les roben información?
Utilizar documentación digital y con una criptografía robusta... aunque creo que ya saben lo que tienen que hacer; lo que pasa es que, a veces, influye el error humano.

¿Trabajas con el Mando de Ciberdefensa? No directamente con ellos, pero sí he estado en algunas reuniones.

¿Te ciberalistarías?
Yo soy objetor de conciencia, pero me preocupa mi país, mi familia, mis amigos…Si fuera necesario, claro que ayudaría.

Qué te queda por aprender
El infinito -risas-. Aquí, en Eleven Paths, hay gente muy buena y compartimos conocimientos cada día. Ellos me cuentan cosas, yo les cuento cosas y tenemos un ritmo de aprendizaje brutal. Pero cada día que me levanto es como si partiera de cero.

¿En el futuro seremos aún más vulnerables?
Tenemos que mejorar mucho en todo. Evidentemente, el que primero tiene que invertir es el Estado, igual que se hace, por ejemplo, en seguridad vial. También hace falta educar a los que han nacido inmersos en la era digital para que obren bien en Internet. Cuando llegué a Telefónica un ejecutivo me preguntó, "¿Hacia dónde va a ir el futuro de Internet?" Pues no tengo ni idea, pero quien seguro que te lo va a decir es tu hijo de ocho o diez años. Las formas que van a tener de relacionarse no van a ser las que tenemos nosotros ni las que tuvieron nuestros padres. Ellos van a decidir qué quieren en el futuro y quizá quieran que se sepa todo de sus vidas a cambio de disfrutar de más relaciones. La generación de nuestros hijos ligará más, pero tendrá una cultura de privacidad muy distinta a la nuestra.



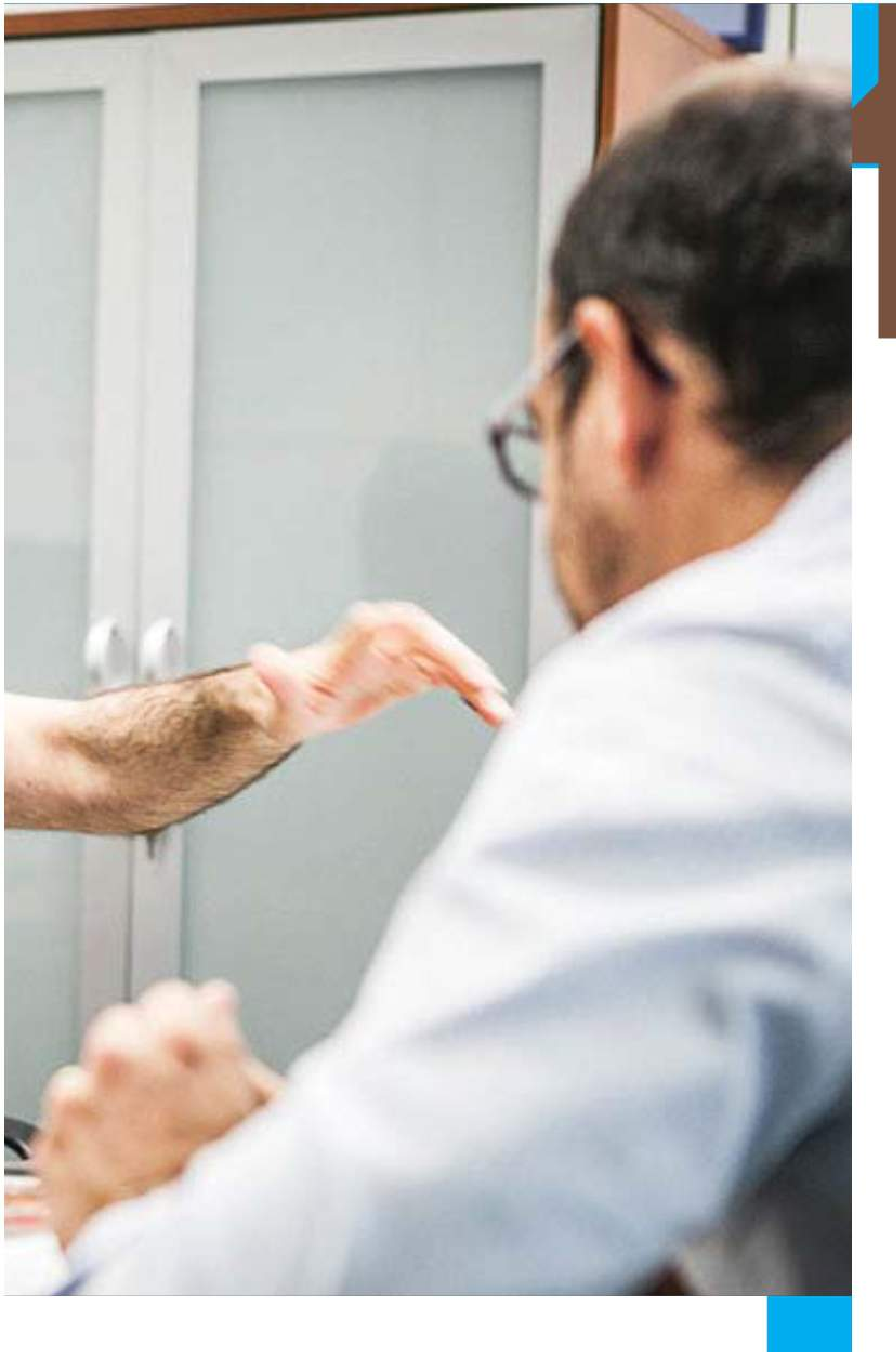
¿Cuántas personas trabajan en Eleven Paths, la compañía que diriges?
Ahora somos casi 60 y estamos integrados en Telefónica para incrementar su potencia a la hora de crear nuevos productos.

¿Y cuántos están bajo tu mando directo? … Casi 60 -risas-. No tengo interacción con todos ellos, pero casi.

¿A quién te gustaría fichar y por qué?
Me gustaría traer a muchos hackers españoles que se han tenido que ir fuera de España. Es una pena que no trabajen aquí.

El reto de Eleven Paths...
Nuestro objetivo es hacer cosas nuevas y disruptivas que no esté haciendo nadie. Ya hemos sacado muchos productos: Metashield, para limpiar los metadatos en entornos empresariales; Faast, que es un sistema de análisis persistente -una auditoría constante los 365 días del año- en el que, desde nuestra 'cloud', atacamos las empresas y vemos si son seguras. Y Lacht, una aplicación móvil que permite





a los usuarios poner un 'pestillo' a su identidad de tal forma que si alguien consigue nuestras claves no puede acceder a nuestro Facebook porque le hemos puesto ese 'pestillo'. Sirve para cualquier persona en Android e iOs. Y este año vamos a presentar muchas novedades más... También es muy interesante Tacyt que permite detectar applicaciones móviles con software malicioso para realizar ciberinteligencia. Estamos desarrollando muchas cosas...

¿Haréis antivirus para la gente?

Hay empresas que son muy buenas en este campo pero nuestro objetivo no es reinventar la rueda sino entender hacia dónde nos va a llevar el mundo y aportar soluciones. Hay mucho por hacer para mejorar la vida de las personas.

Tu sueño es inventar....

Estoy contento con lo que he hecho: con la información que sé y que aprovecho para hablar de vulnerabilidades, con los programas para proteger tu información y saber si te han ciberatacado, como FOCA -Fingerprinting Organizations with Collected Archivs- para hacer auditorías de seguridad informática-, con Lacht -que me gusta mucho- y con Tacyt o Sinfonier...

CONFIDENCIAS

ASÍ LLEGUÉ A CONVERTIRME EN HACKER

Si eres un adolescente y estás "perdido"... es normal. Desde que empecé a mantener más en serio los contenidos de mi Canal Youtube, una buena cantidad de jóvenes, más aficionados al vídeo que al RSS de lectura, se han puesto en contacto conmigo. Chicos y chicas de entre 15 y 20 años que están indecisos sobre su futuro, o sobre a qué dedicarse, o sobre cuáles son las prioridades en su vida. Es para ellos para los que escribo este artículo.

Recuerdo que toqué mi primer ordenador cuando tenía 12 años. Recuerdo que fue ver la película de TRON y enamorarme para siempre de la programación. Me apunté a una academia de barrio -que hace años cerró- y ya sabía algo. Adoraba la informática y me encantaba estar aprendiendo siempre cosas.

Aunque paso muy a menudo por delante de la academia en cuestión, para poder ver el local exacto donde se encontraba el aula en la que por primera vez escribí eso de 5 CLS, un fin de semana me quedé mirándola y le tiré una foto. He pasado tantas veces por delante que no me había dado cuenta de lo "zulo" que era. Sin ventanas, sin luz, parece un almacén. Pero ahí estaban los Amstrad, los dragones, los Sinclair, etc...

Me quedé un rato pensando en cómo, desde aquel día hasta hoy, el camino me había llevado a estar ligado a la informática. Y recordé que no siempre lo tuve tan claro. Sí, es cierto que lo tuve claro con 12 años y también que lo tuve claro con 20 años, pero en una época difícil llamada adolescencia, no lo tuve tan claro... y me perdí en otras cosas.

Me perdí en los botellones. Me perdí en las "acampedos". Me perdí en los conciertos de música cuanto más salvajes mejor. Me perdí en las partidas de mus en el bar y los cigarros al son de una guitarra en unas escaleras. Me perdí en las cañas y los partidos de fútbol en la tele con los amigos. Me perdí en vicios de adolescente que está descubriéndose a sí mismo y el mundo. Y podría haber salido mal.... claro que sí, pero solo fue una fase -y que no recuerdo como algo malo, sino como algo circunstancial-.

De hecho, hubo una época en la que tener algo de dinero más en el bolsillo era más importante que estudiar. En la que tomarse una cerveza más tenía prioridad sobre programar y en la que quedar con chicas era más importante que los estudios. Sí, era un adolescente normal y corriente del montón.

Luego... me centré. No sé si por la edad, por mi situación personal, porque incluso mis amigos me decían que tenía que seguir estudiando ya que era buen estudiante o porque encontré en mi amigo Rodol - con el que acabaría montando Informática 64- un compañero con el que seguir alimentando mi pasión por la informática.

No sé cuál fue el motivo. Supongo que sería contar con una madre que siempre me apoyaba y empujaba a seguir, o con una necesidad imperiosa de buscarme la vida, con un amigo con el que hacía piña en el mundo de la informática - aunque fuera jugando al Quake por teléfono en el año 1997, o hablando de cómo actualizar el firmware de su route o cómo gaitas liberábamos más memoria para que pudiera cargar un programa-, o simplemente casualidad, destino o la suma de todo un poco. Con 12 años me enamoré, y con 20 me di cuenta de que seguía enamorado de los ordenadores.

Si estás perdido ahora, y tienes las prioridades en otro lado, no te flageles. Puede que aún seas un adolescente y estés como estaba yo. Intenta centrarte poco a poco y no olvides aquello que cuando tenías 10 u 11 años querías ser y amabas. Cuando sepas lo que quieres hacer, comienza a trabajar en esa dirección. Aprovecha tu tiempo y te convertirás en lo que quieras ser. No pienses que no puedes. Tú puedes como cualquiera de los demás, que no hay cosas difíciles, sino que hay que trabajarlas. ¡Ánimo!

Puedes seguir a Chema Alonso en elladodelmal.com

CONVIÉRTETE EN UN EXPERTO

¿QUIERES SER COMO CHEMA ALONSO?

MÁSTER UNIVERSITARIO EN SEGURIDAD INFORMÁTICA

QUIÉN: Universidad Internacional de la Rioja -UNIR-.
DÓNDE: Online.
CUÁNDO: De marzo a diciembre
QUÉ: Los alumnos, una vez realizan el máster, adquieren las principales técnicas de protección frente a ataques y a amenazas en sistemas operativos, redes, software de aplicaciones, sistemas web y bases de datos. Asimismo, señalan desde UNIR que al salir se tienen las "competencias necesarias para la gestión, análisis de riesgos y auditoría de la seguridad de las tecnologías de la información" en cualquier organización.
MATRÍCULA: 5.900€.
+ INF: http://www.unir.net/ingenieria/master-seguridad-informatica/549200001557/

MÁSTER EN BIG DATA Y BUSINESS ANALYTICS

QUIÉN: Centro Internacional de Formación Financiera (CIFF), Universidad de Alcalá de Henares.
DÓNDE: Centro de Formación de CIFF en Madrid (C/ María de Molina 27).
CUÁNDO: De noviembre a julio
QUÉ: Busca dar respuestas a las necesidades de análisis de datos de las compañías a través de un programa que gira en torno a ocho módulos centrales en los que se aprende, entre otras materias, herramientas y técnicas de análisis o gestión de datos.
MATRÍCULA: 10.200€.
+ INF: http://www.ciff.net/master-en-big-data-y-business-analytics.html#

MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD

QUIÉN: Universidad Carlos III, Madrid.
DÓNDE: Ronda de Toledo, 1; CP: 28005 Madrid.
CUÁNDO: De septiembre a junio.
QUÉ: Está pensado para aquellos que quieran ser ingenieros de sistemas seguros o analistas de ciberseguridad. A pesar de que hay dos itinerarios para diferenciar los perfiles, en ambos casos se aprende a usar herramientas comunes para los ciberataques y la ciberdefensa. Muchas de las asignaturas son en inglés.
MATRÍCULA: 4.810,2€ los estudiantes de la UE -6.000€ para los de fuera-.
+ INF: http://www.uc3m.es/ss/Satellite/Postgrado/es/io_C/1371209197821/1371208956904/Master_Universitario_en_Ciberseguridad

CYBERSECURITY MANAGEMENT

QUIÉN: Universitat Politècnica de Catalunya.
DÓNDE: Tech Talent Center. C/ de Badajoz, 73-77, Barcelona.
CUÁNDO: De octubre a julio.
QUÉ: Hacking ético, Data Mining, análisis de malware, gobierno de la seguridad o amenazas y criptografía son algunos de los temas que se abordarán en el máster. Aquellos que se apunten podrán optar a dos certificaciones ISACA, reconocidas a nivel internacional.
MATRÍCULA: 8.000€.
+ INF: http://www.talent.upc.edu/esp/professionals/presentacio/codi/221100/cybersecurity-management/

MÁSTER PROFESIONAL EN TECNOLOGÍAS DE LA SEGURIDAD

QUIÉN: Universalidad de León -ULE-
DÓNDE: Escuela de Ingenierías Industrial e Informática, Campus de Vegazana, s/n; Universidad de León.
CUÁNDO: De noviembre a julio.
QUÉ: Está dividido en tres bloques. En el primero, denominado "General", se abordan asuntos como las redes de Sistemas TIC y la Seguridad o el desarrollo y la programación seguras; en el segundo, llamado "Seguridad de sistemas", se trata la seguridad en redes, los sistemas complejos robustos o la configuración para servicios seguros; y, en el tercero, bajo el título de "Auditorías de seguridad y análisis forense", los temas centrales son análisis forense, auditoría y análisis de 'malware' y 'reversing'.
MATRÍCULA: 2.150€.
+ INF: http://masterseguridad.unileon.es/

¿HAS DECIDIDO ADENTRARTE EN EL APASIONANTE MUNDO DE LA CIBERSEGURIDAD... PERO NO TIENES MUY CLARO EN QUÉ ESPECIALIZARTE? AQUÍ TE RECOMENDAMOS ALGUNOS MÁSTERS IMPRESCINDIBLES PARA TU DESARROLLO ACADÉMICO. ESO SÍ, NECESITAS TENER ESTUDIOS SUPERIORES UNIVERSITARIOS PREVIOS, RELACIONADOS CON LAS TELECOMUNICACIONES O LA INFORMÁTICA. TEXTO BORJA G. DE SOLA

MÁSTER INTERNACIONAL EN CIBERSEGURIDAD Y CIBERDEFENSA

QUIÉN: Campus Internacional de Seguridad y Defensa -CISDE-. Fundación San Pablo Andalucía CEU.
DÓNDE: Online.
CUÁNDO: De noviembre a julio.
QUÉ: Destinado a profesionales de la seguridad informática, cuerpos y fuerzas de seguridad del Estado y militares de carrera, el objetivo es formar al alumno en profundidad acerca de posibles ataques cibernéticos.
MATRÍCULA: 1.995€.
+ INF: http://cisde.es/catalogo-de-cursos/masters/master-internacional-en-ciberseguridad-y-ciberdefensa-2

MÁSTER INDRA EN CIBERSEGURIDAD

QUIÉN: Indra y U-Tad, Centro Tecnológico de Tecnología y Arte Digital.
DÓNDE: Sede de la U-Tad, Parque Europa Empresarial - C/. Playa de Liencres, 2 duplo - Edificio Madrid – 28290. Las Rozas, Madrid.
CUÁNDO: De octubre a julio.
QUÉ: Este máster está enfocado a la formación, técnica y táctica, de "ciberdefensa, ciberataque, análisis forense de sistemas informáticos, estudio y análisis de seguridad de dispositivos móviles y sistemas de control industrial". Asimismo, los alumnos llevarán a cabo sesiones de entrenamiento práctico en el Simulador Avanzado de Ciberseguridad iPhalax de Indra -cyber range-.
MATRÍCULA: 11.860€.
+ INF: https://www.u-tad.com/estudios/master-indra-en-ciberseguridad/

MÁSTER EN CIBERSEGURIDAD UCAV - DELOITTE

QUIÉN: Universidad online de Ávila.
DÓNDE: Online.
CUÁNDO: De enero a septiembre
QUÉ: Este máster busca ampliar los conocimientos en "seguridad informática, hacking, auditorías de seguridad de sistemas de información, desarrollo seguro de aplicaciones, gestión de alertas de seguridad, etc.". Además, con este título puedes obtener también la certificación de Hacking Ético -ver página 74- y Desarrollo Seguro.
MATRÍCULA: Unos 5.300 euros
+ INF: http://online.ucavila.es/master-ciberseguridad-deloitte?piloto=av23

MÁSTER EN GOBIERNO DE LA CIBERSEGURIDAD

QUIÉN: ISMS Fórum y la Universidad Politécnica de Madrid.
DÓNDE: Avenida Complutense 30, Ciudad Universitaria, Madrid, E.T.S.I. Telecomunicación-U.P.M.
CUÁNDO: De octubre a julio
QUÉ: Pensado para que directivos relacionados con el mundo de las Tecnologías de la información y la comunicación, ingenieros, consultores o profesionales interesados en la c iberseguridad profundicen sus conocimientos sobre esta materia. Los alumnos aprenderán cuáles son los modelos de ciberseguridad, cómo implementar sistemas de gestión de seguridad y serán capaces de descubrir los riesgos relacionados con la ciberseguridad en una empresa u organismo público.
MATRÍCULA: 7.900€ para los asociados de ISMS Fórum y 8.950€ para los no asociados.
+ INF: https://www.ismsforum.es/curso/27/master-en-gobierno-de-la-ciberseguridad/

SI TE GUSTA LA INFORMÁTICA, TE ESTÁN BUSCANDO...

¿Quieres trabajar en CIBERSEGURIDAD?

EMPRESAS Y ORGANISMOS PÚBLICOS NECESITAN CUBRIR UN MILLÓN DE PUESTOS DE TRABAJO EN EL ÁMBITO DE LA SEGURIDAD DE LA INFORMACIÓN, SEGÚN EL EXPERTO DE TREND MICRO, LOÏC GUÉZO. SI TE GUSTA ESTE MUNDO Y CREES QUE ESTÁS PREPARADO PARA DAR EL SALTO, **ESTE ES EL TOP 20 DE COMPAÑÍAS EN LAS QUE TIENES QUE ECHAR EL CURRÍCULUM.** HAY DESDE MULTINACIONALES EXTRANJERAS HASTA NUEVAS EMPRESAS ESPAÑOLAS.

LOS MEJORES TRABAJOS PARA LUCHAR CONTRA LOS HACKERS DEL MAL

"En seguridad informática hay tres grandes ramas: la técnica -hacker ético-, la normativa -los que se dedican a diseñar los procesos de seguridad, accesos, medios que hay que tener- y seguridad física -son los encargados de regular los accesos físicos y virtuales a un ordenador, un sistema, un determinado programa, etc.-", explica el consultor senior en selección de personal para perfiles informáticos de Hays, Julien Mur, que desvela los trabajos en alza en este sector.

1 HACKER ÉTICO

Es el trabajo más famoso y reconocido. Se trata del profesional experto en acceder a todo tipo de sistemas -siempre de forma legal- a través de sus vulnerabilidades -errores en los sistemas que pueden ser aprovechados para acceder a ellos-. En 2005, por ejemplo, una empresa de seguridad llamada TippingPoing, comenzó a ofrecer recompensas por este tipo de información y desde entonces ha pagado a más de 1.600 personas que le han facilitado las llamadas 'vulnerabilidades Zero Day' -ver página 9-. También es conocido el caso de un hacker de Shanghai, Wu Shi, que ha ganado más de 280.000 euros informando a las compañías de navegadores de más de un centenar de vulnerabilidades. En España, varios hackers de reconocido prestigio imparten conferencias y asesoran a empresas analizando su seguridad de la información. Este año, compañías como Google o Microsoft han anunciado que para mejorar su tecnología ofrecerán importantes 'recompensas' a quienes informen de las vulnerabilidades y técnicas de explotación de sus programas. Por ejemplo, en el caso de Microsoft, se ha ofrecido a pagar hasta unos 93.000 euros a quienes le informen de fallos de seguridad en su sistema operativo Windows.

NECESITAS ESTUDIAR: Máster en seguridad informática

COBRARÁS: Entre 35.000 y 45.000 €/año, según experiencia.

2 CONSULTOR DE SEGURIDAD INFORMÁTICA

Es la persona que va realizar tests de vulnerabilidades y pruebas de acceso. Se encarga, mediante ensayos automatizados, de ver que no existen formas de acceder a la información sensible de la empresa en diferentes niveles de seguridad. También conoce qué normativa hay que aplicar y la traslada a la empresa.

NECESITAS ESTUDIAR: Ingeniería informática o máster de seguridad de la información.

COBRARÁS: Entre 34.000 y 50.000 €/año, para los que tienen de dos a diez años de experiencia.



3 RESPONSABLES DE SEGURIDAD INFORMÁTICA

Es el jefe del hacker ético y de los consultores. Se le conoce también por el nombre CISO -Chief Information Security Officer-. También lleva el presupuesto que hay que dedicar a proteger la información en cada empresa.

NECESITAS ESTUDIAR: Ingeniería informática

COBRARÁS: De 80.000 a 120.000 €/año, según experiencia.

4 PROJECT MANAGER

Es un puesto ejecutivo en el que se trabaja para una consultora tecnológica o de seguridad informática, realizando proyectos para terceros. Se sienta con el cliente y se encarga de cubrir sus necesidades: seguridad propia, de sus productos, vigilancia ante amenazas…

NECESITAS ESTUDIAR:

Ingeniería informática y certificaciones informáticas de diferentes conocimientos –CIFFP o CEH-.

COBRARÁS: De 30.000 a 40.000 €/año.

5 CDO -CHIEF DATA OFFICER-

Es el responsable de los datos de una empresa, incluyendo el almacenamiento de la base. Decide si se debe fichar a un encargado de seguridad. Es uno de los trabajos más 'jóvenes' del mercado –tiene unos cuatro años-.

NECESITAS ESTUDIAR: Máster en seguridad de la información, MBA o ingeniería informática.

COBRARÁS: Desde 100.000 €/año.

6 EXPERTO EN VULNERABILIDADES

Se trata de expertos en encontrar vulnerabilidades en todo tipo de programas. Algunos trabajan para consultoras que, a su vez, trabajan para empresas. También existen 'freelance' que venden a las empresas los problemas que encuentran –incluso pueden ser contratados para ver si el ordenador del CEO de la empresa es o no vulnerable-.

NECESITAS ESTUDIAR: Ingeniería Informática.

COBRARÁS: Hasta medio millón de euros por una vulnerabilidad 'zero day'.

Dónde enviar tu currículum



SYMANTEC

ORIGEN: Fundada en 1982 por Gary Hendrix.
SEDE PRINCIPAL: Mountain View, California, Estados Unidos.
QUÉ HACE: Se dedica a desarrollar software de seguridad informática. Su producto más conocido es Norton Antivirus.
CONTACTA: symantec.com/es/es/about/careers/



BT

ORIGEN: 1846.
SEDE PRINCIPAL: Londres, Reino Unido.
QUÉ HACE: Esta multinacional británica, que se dedica a proporcionar servicios de comunicaciones y tecnologías de la información a compañías y organismos públicos, también ofrece soluciones de seguridad a más de 1.000 empresas en 170 países. Fueron los encargados de proteger los últimos Juegos Olímpicos.
CONTACTA: www.bt.es

BUGUROO

ORIGEN: 2010
SEDE PRINCIPAL: La Moraleja, Madrid, España.
QUÉ HACE: Es una de las pocas empresas españolas que fabrican software para ofrecer soluciones de seguridad a otras compañías. Su compromiso es "detectar, evaluar y actuar".
CONTACTA: buguroo.com – trabaja con nosotros



GMV

ORIGEN: 1984.
SEDE PRINCIPAL: Tres Cantos, Madrid, España.
QUÉ HACE: Con más de 15 años de experiencia en el desarrollo de soluciones de ciberseguridad, GMV analiza y diagnostica entornos para determinar los posibles riesgos, elabora planes para proteger, por ejemplo, infraestructuras críticas, ofrece soluciones tecnológicas de seguridad...
CONTACTA: gmv.com/es/Empleo

NECSIA

ORIGEN: 2005. El 100% del capital es español.
SEDE PRINCIPAL: Barcelona, España.
QUÉ HACE: Su objetivo es que las grandes compañías españolas sean "más seguras, eficientes y colaborativas". ¿Cómo pretenden conseguirlo? A través de sus servicios de auditoría, consultoría y soluciones.
CONTACTA: necsia.es/trabajar-en-necsia



PROSEGUR

ORIGEN: Nace en 1976 de la mano de Herberto Gut Beltrán.
SEDE RINCIPAL: Madrid, España.
QUÉ HACE: Cuenta con varios Centros Globales de Operaciones de Seguridad, expertos en seguridad de la información y alianzas con partners tecnológicos para ofrecer servicios de ciberseguridad "con garantías".
CONTACTA: prosegur.es/esp/talento-prosegur/index.htm



KPMG

ORIGEN: Llega a España en 1971.
SEDE PRINCIPAL: Ámsterdam, Países Bajos.
QUÉ HACE: Asesora a los clientes para que sean capaces de detectar, prepararse y protegerse ante un ataque. Considera que el ámbito de la ciberseguridad está a la vanguardia tecnológica, motivo por el cual en junio compró Zink Security, especializada en vigilancia digital.
CONTACTA: home.kpmg.com/es/es/home/carreras/ofertas-de-empleo.html



ATOS

ORIGEN: Surge en 1997, fruto de la fusión de Axime y Sligos.
SEDE PRINCIPAL: Bezons, Francia.
QUÉ HACE: Su estrategia es que sus clientes sepan gestionar los riesgos de la ciberseguridad para que "vean las oportunidades del mercado", como la nube o el 'Bring your own device' –política empresarial en la que los empleados acceden a la información corporativa con sus dispositivos personales–.
CONTACTA: es.atos.net/es-es/home/empleo/ofertas-de-empleo.html



HEWLETT PACKARD

ORIGEN: 1939.
SEDE PRINCIPAL: Palo Alto, California, Estados Unidos.
QUÉ HACE: Es uno de los principales "proveedores de soluciones de ciberseguridad para organizaciones de defensa e inteligencia". Se encarga de la intranet de la Marina y el Ejército estadounidense, así como de la infraestructura de información de Defensa del Reino Unido.
CONTACTA: http://www8.hp.com/us/en/jobs/working-at-hp.html



ORACLE

ORIGEN: Fundada en 1977, con el nombre Software Development Laboratories
SEDE PRINCIPAL: Redwood Shores, California, Estados Unidos.
QUÉ HACE: A través del Oracle Information Security ayuda a las empresas a que sus sistemas de negocio críticos estén disponibles de una forma segura. La ciberdefensa también tiene un papel muy importante.
CONTACTA: https://www.oracle.com/corporate/careers/index.html



MICROSOFT

ORIGEN: En 1975, Bill Gates y Paul Allen crearon uno de los mayores gigantes tecnológicos de la historia.
SEDE PRINCIPAL: Redmond, Washington, Estados Unidos.
QUÉ HACE: Microsoft acaba de crear el Centro de Operaciones de Ciberdefensa y el Grupo de Ciberseguridad Empresarial para proteger los datos de los consumidores. El primero está formado por expertos de la compañía y tiene como misión principal "proteger, detectar y responder a las amenazas en tiempo real", mientras que el Grupo buscará entregar soluciones de seguridad, experiencia y servicios para que las empresas modernicen sus plataformas de Tecnologías de la Información, migren a la nube de forma segura y mantengan sus datos a salvo.
CONTACTA: https://www.microsoft.com/es-es/learning/explore-jobs.aspx

OTRAS EMPRESAS QUE TAMBIÉN DEBES TENER MUY EN CUENTA:

Accenture: www.accenture.com/es-es/careers/jobsearch
Iecisa (El Corte Inglés): www.iecisa.com/web/es/ofertas-activas
Sophos: www.sophos.com/es-es/about-us/careers/spain.aspx
S21sec: www.s21sec.com/es/sobre-s21sec/trabaja-con-nosotros



INDRA

ORIGEN: 1993. El Estado español es su mayor accionista a través de la SEPI que tiene un 20% de su capital.
SEDE PRINCIPAL: Alcobendas, Madrid, España.
QUÉ HACE: La firma española tiene tres objetivos claros a la hora de proteger en materia de ciberseguridad a particulares, organismos –públicos y privados– e infraestructuras críticas. Primero, minimizar las vulnerabilidades de los sistemas de Tecnologías de la Información y Comunicación -TIC-; segundo, proteger la información que dependa de los sistemas TIC; y, tercero, asegurar el negocio y el servicio al cliente de las empresas que la han contratado.
CONTACTA: http://www.indracompany.com/tu-carrera-en-indra/empleo-en-indra

DELOITTE

ORIGEN: 1845. Su creador fue William Welch Deloitte.
SEDE PRINCIPAL: Nueva York, Estados Unidos.
QUÉ HACE: Su misión principal es ayudar a las organizaciones que contratan sus servicios a "preparar, conocer y responder" ante las ciberamenazas. Preparar se refiere a que todos los trabajadores entiendan los riesgos y las consecuencias de un ciberataque; conocer es identificar y comprender qué persigue un ataque haciendo un seguimiento a las tendencias en las amenazas; y responder tiene relación con la capacidad de reacción de la empresa –ser capaz de frenar el impacto de un ciberataque y analizar las consecuencias-.
CONTACTA: careers.deloitte.com/jobs/spa-es?icid=top_job-search

IBM

ORIGEN: Se funda en 1911, fruto de la fusión de cuatro empresas. Su principal accionista es Berkshire Hathaway, de Warren Buffet, con un 8,2%.
SEDE PRINCIPAL: Nueva York, Estados Unidos.
QUÉ HACE: IBM lleva a cabo consultoría de ciberseguridad en la que evalúa si los controles de seguridad de las empresas que son sus clientes funcionan bien y les ofrece recomendaciones a corto, medio y largo plazo. Asimismo, desde IBM educan a sus clientes para que conozcan las directrices para identificar y priorizar los riesgos a los que se enfrentan
CONTACTA: www-05.ibm.com/employment/es/

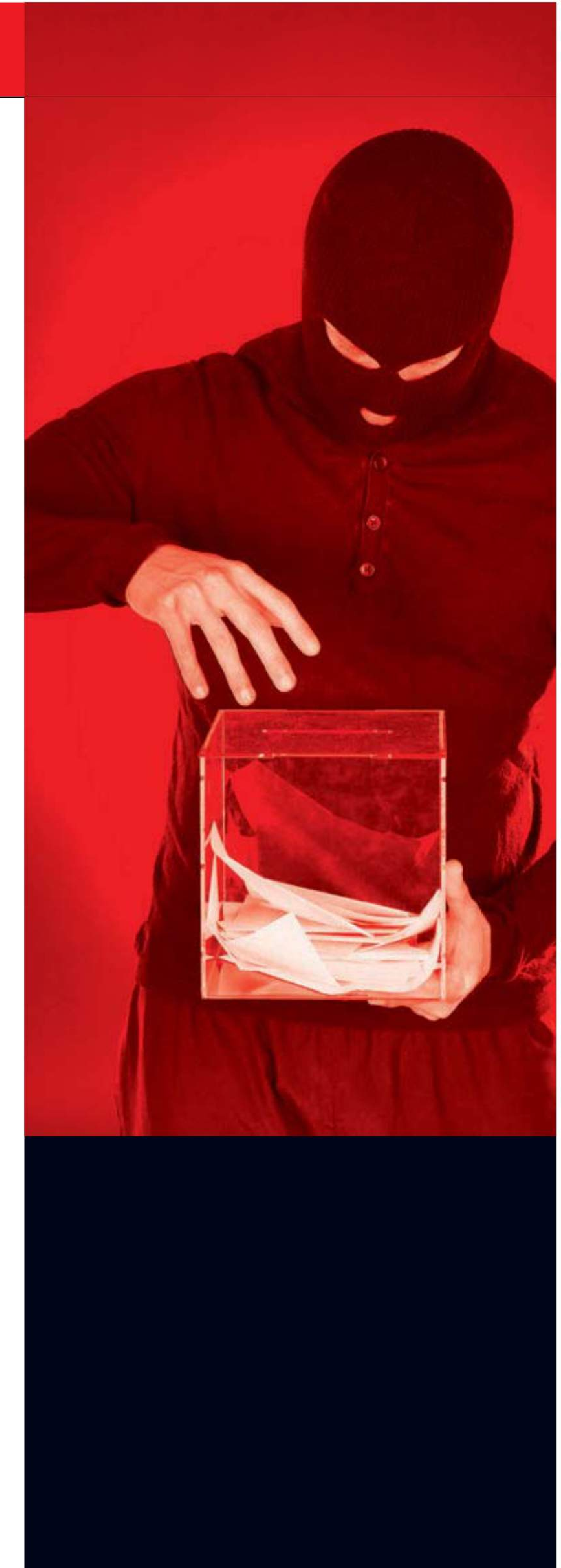
INTEL

ORIGEN: 1968.
SEDE PRINCIPAL: Mountain View, California, Estados Unidos.
QUÉ HACE: Para proteger sus chips –Intel es el principal fabricante del mundo– de posibles hackeos, la multinacional estadounidense invierte cada año millones de euros en ciberseguridad. Asimismo, desde 2014 es propietaria de la compañía de software de seguridad Intel Security Group, conocida anteriormente como McAfee.
CONTACTA: intel.com/content/www/us/en/jobs/jobs-at-intel.html

ELEVEN PATHS

ORIGEN: 2013. Pertenece a Telefónica.
SEDE PRINCIPAL: Madrid, España.
QUÉ HACE: Según la propia empresa, se dedican a crear productos innovadores que vayan por delante de los atacantes y que transformen el concepto actual que hay de seguridad. Para hacer frente a las amenazas tienen cuatro servicios: Faast –una tecnología de penetración que escanea en todo momento el sistema informático–; Metashield –para protegerse contra la fuga de datos e información–; Sinfonier –que detecta ciberamenazas haciendo procesamientos de información en tiempo real–; y Tacyt, una herramienta de ciberinteligencia de amenazas para móvil
CONTACTA: wearehiring@11paths.com

CÓMO SE PROTEGEN LOS SISTEMAS DE VOTO Y RECUENTO ON LINE ¿ES POSIBLE AMAÑAR LAS ELECCIONES EN ESPAÑA?



En las elecciones generales de 2015, el recuento de los millones de votos y el posterior envío de esos resultados se realiza a través de Internet, con la tecnología más avanzada. Un escenario 'perfecto' para que los ciberdelincuentes intenten 'hackear' los resultados provisionales... Y esto es algo que ya ha sucedido. // Texto: Elisa Coello

Son las ocho de la tarde del domingo de las elecciones generales y 22.951 colegios y centros electorales cierran sus puertas en toda España después de una intensa jornada de votaciones. Cerca de 36,5 millones de habitantes censados desean conocer los resultados. El recuento de votos mantendrá, otra vez, a todos ellos en vilo, a la espera de los primeros datos del escrutinio. Pero, esta vez, alguien podría 'reescribir las reglas' desde el teclado de su ordenador.

Para tranquilidad de muchos, de momento, en España no está implantado el voto electrónico -para votar por Internet- tal y como sucede en países como Estados Unidos, Brasil o Venezuela. Sin embargo, sí que se remiten los resultados de las votaciones de cada mesa al centro de recogida de datos de los comicios através de Internet -que los remite, de igual forma, a los medios de comunicación-. Un sistema que, hasta el momento, no ha resultado totalmente seguro...





CUÁNTA GENTE VOTA EN ESPAÑA

Más de 36,5 millones de ciudadanos pueden votar en las elecciones a las Cortes Generales. Para depositar su voto disponen de 57.486 mesas electorales distribuidas en 22.951 colegios y centros habilitados.



VOTACIÓN A DISTANCIA POR CORREO

En la actualidad, 1.875.272 españoles residentes en el extranjero tienen derecho a votar, según el Instituto Nacional de Estadística. Como curiosidad, en 2015 es la segunda vez que la solicitud para ejercer el voto desde fuera de España se puede hacer por Internet. En las últimas elecciones municipales y locales, en mayo de 2015, algo más de 600.000 personas votaron desde el extranjero. También pueden votar por correo aquellos que, residiendo en España, no puedan o no quieran hacerlo de forma presencial.



CONSULTA AQUÍ todo sobre las elecciones

TRABAJO EXTRA PARA LOS CIBERAGENTES

Si la intención de los hackers de sombrero negro o 'blackhat hackers' -criminales que vulneran la seguridad informática con fines maliciosos- es sabotear los comicios, manipular o destruir los resultados o hacer quedar en evidencia a las altas esferas, es más que probable que encuentren una brecha; es lo único que necesitan. Ya pueden enfrentarse a los servidores más avanzados, los terminales más punteros o la última tecnología en transmisión de datos, que siempre puede existir una vulnerabilidad -en último caso, el factor humano- que permita alterar el censo electoral o el envío de la información con el recuento de votos. Prueba de la facilidad para atacar este tipo de sistemas es el caso de EE.UU., donde se dio a conocer que la llave que daba acceso a la 'SmartCard' -tarjeta de memoria que registra la votación on line- se podía falsificar a partir de una simple foto. Es más: hubo hackers que demostraron en un congreso de ciberseguridad -el Black Hat- que esta llave servía también para acceder... ¡al mueble-bar del hotel donde se alojaban!

¿Por qué interesan los fallos que se hayan detectado en las máquinas con las que votan los estadounidenses? La respuesta es sencilla. Mucha de la tecnología usada en nuestro país proviene de Estados Unidos, que es donde se encuentran las pocas empresas que se dedican a desarrollar estos dispositivos informáticos, tanto

En España se han producido varios fallos electrónicos el día de las elecciones

para registrar el voto como para enviar los resultados.


De hecho, en las últimas elecciones generales celebradas en España, en noviembre 2011, la página de Teletexto de RTVE publicó durante varios minutos los datos erróneos, proporcionados por Indra, que proclamaban al PSOE ganador con 166 escaños, frente a los 108 del Partido Popular -que fue el ganador final-. Además, la tercera fuerza, según estos datos.... ¡fue el Partido Anticapitalista! RTVE se excusó alegando que los datos utilizados son comunes para todos los medios de comunicación, porque hay una única fuente que los suministra... aunque ellos fueron los únicos que se equivocaron. Los resultados fueron corregidos rápidamente, pero las redes sociales ya se habían hecho eco del patinazo. Y no ha sido la única vez donde el último eslabón del proceso fue vulnerado...

INDRA, MÁXIMA SEGURIDAD

Los resultados de las penúltimas elecciones autonómicas en España, celebradas en mayo de 2011, sufrieron un retraso a la hora de llegar a los medios de comunicación ¿La razón? La empresa encargada del suministro de los datos de los escrutinios, Indra, pudo sufrir un fallo de denegación de servicio distribuido en su servidor. ¿Qué significa esto? La página de resultados que nutría a todos los medios españoles no pudo hacer su trabajo como se esperaba durante el período de recuento de votos, al parecer, por múltiples problemas técnicos simultáneos que impidieron la difusión de los resultados. Si el fallo fue por sobrecarga del sistema o por un ataque masivo, no lo sabemos -la compañía nunca lo ha aclarado-. Lo que sí está claro es que si fue debido a la saturación del servidor también podría haber sido vulnerable a un ataque externo. El resultado es que los diarios digitales -los primeros que publican resultados a esas horas de la noche- tuvieron que trabajar con datos sin actualizar durante varias horas, hasta que se solucionó el problema. La peculiaridad de las elecciones municipales y autonómicas es que, al estar más distribuidas, existe la posibilidad de que algunas comunidades se desmarquen y decidan utilizar una tecnología alternativa para el suministro de los datos.

MAL DEBUT DEL VOTO ELECTRÓNICO

En las elecciones al Parlamento catalán de noviembre de 2010, todos los ciudadanos con derecho a voto tuvieron la oportunidad de probar, por primera vez en nuestro país, la experiencia piloto de votar desde su teléfono móvil. El voto se realizaba, además del modo presencial, mediante acreditación del elector con un código que recibía



previamente por mensaje de texto. Hubo fallos tanto de sobrecarga del servidor que recogía los datos, como en la aplicación que daba acceso a la votación. Incluso el servicio de atención al cliente se colapsó. El fracaso fue importante y provocado, según las autoridades, por una saturación del sistema. De todo lo expuesto, lo que queda patente es que tanto en España como en otros países, todos los elementos puramente tecnológicos que podrían intervenir en el sistema de votación, han sido puestos a prueba... y han evidenciado, en mayor o menor medida, que no son seguros al 100%. ¿El reto? Conseguir un procedimiento inexpugnable que permita identificar, sin dudas, a cada votante y garantice que el número de votos y su recuento no se pueden alterar de forma remota cuando se notifican a la Junta Electoral y al Ministerio de Interior.

Para las elecciones generales de diciembre de 2015 no se emplea el voto electrónico, pero quizá para las siguientes, previstas en 2019, se implante en España este novedoso sistema; sólo es de esperar que para entonces tengamos las medidas de seguridad necesarias para evitar ataques maliciosos. Sin olvidar la máxima más importante en el mundo de la seguridad:"Toda cadena es tan fuerte como el más débil de sus eslabones".

LOS HACKERS PUEDEN TOMAR EL CONTROL DE TU COCHE

Que un hacker decida colarse en tu ordenador puede acarrearte consecuencias muy molestas, pero... si consigue infiltrarse en tu coche, tu seguridad física puede estar en juego. // *Texto: P. Parada*

El claxon empieza a sonar, las luces se apagan de repente en medio de una autopista por la noche, los frenos se activan, la dirección del coche gira sin que toques el volante, las puertas se bloquean… "Con la incorporación masiva de la electrónica al mundo del automóvil -y su cada vez mayor conexión a Internet- han aumentado los riesgos de que tu vehículo pueda ser pirateado", explica el responsable de ciberseguridad de BT Security en España, Francisco José Pereiro, quien recuerda que se puede acceder a muchos sistemas de nuestro coche a través del sistema de conexión inalámbrica Bluetooth o, simplemente, insertando en el equipo de sonido un CD de música infectado. Hay que tener en cuenta que se puede modificar desde la telemetría de los sistemas del coche hasta los sensores que recogen y envían datos para que las centralitas que se encargan de activar los distintos sistemas según la información que reciben, tomen decisiones erróneas: por ejemplo, no desconectar el sistema de suministro de combustible del motor en caso de accidente para evitar un incendio". Sin embargo, de momento, es algo poco probable ya que se tendría que hacer por Bluetooth, y eso exigiría que el hacker estuviera muy cerca, con el consiguiente riesgo de que le descubrieran. Sin embargo, según la consultora Ernst & Young, se espera que, en 2025, más de 100 millones de coches tengan algún tipo de conectividad a Internet... algo que aumentará el riesgo de ser ciberatacados.

■ CASO REAL

Expertos en seguridad han hackeado coches de las marcas Jeep, Toyota, Chevrolet, etc. para demostrar que ningún vehículo es impenetrable y que, de no cuidar la seguridad, las consecuencias pueden ser muy graves. Un juez inglés prohibió en julio de 2013 la publicación de un informe en el que se contaba cómo hackear un Volkswagen al entender que podía ser usado por criminales.

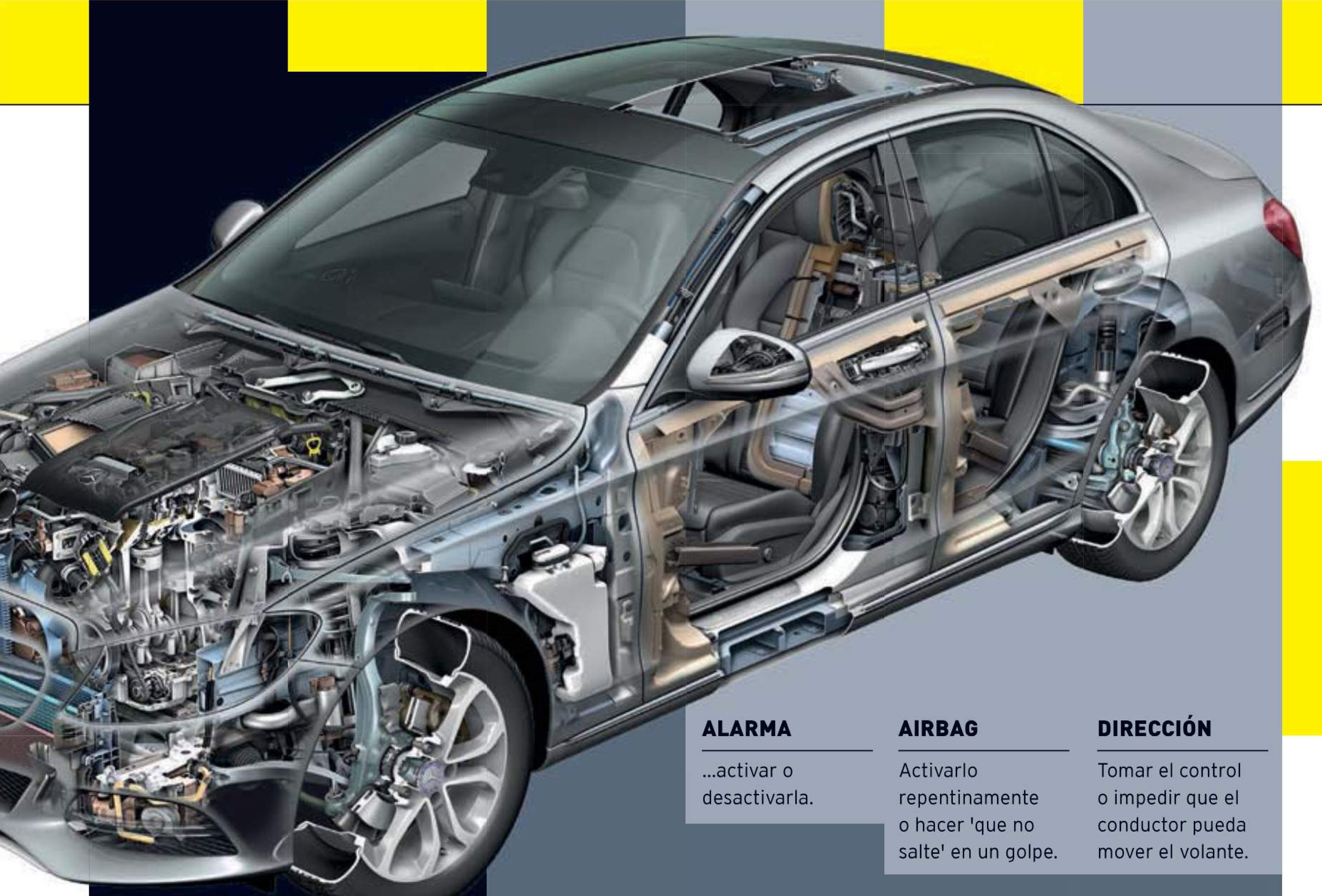
■ CÓMO EVITARLO

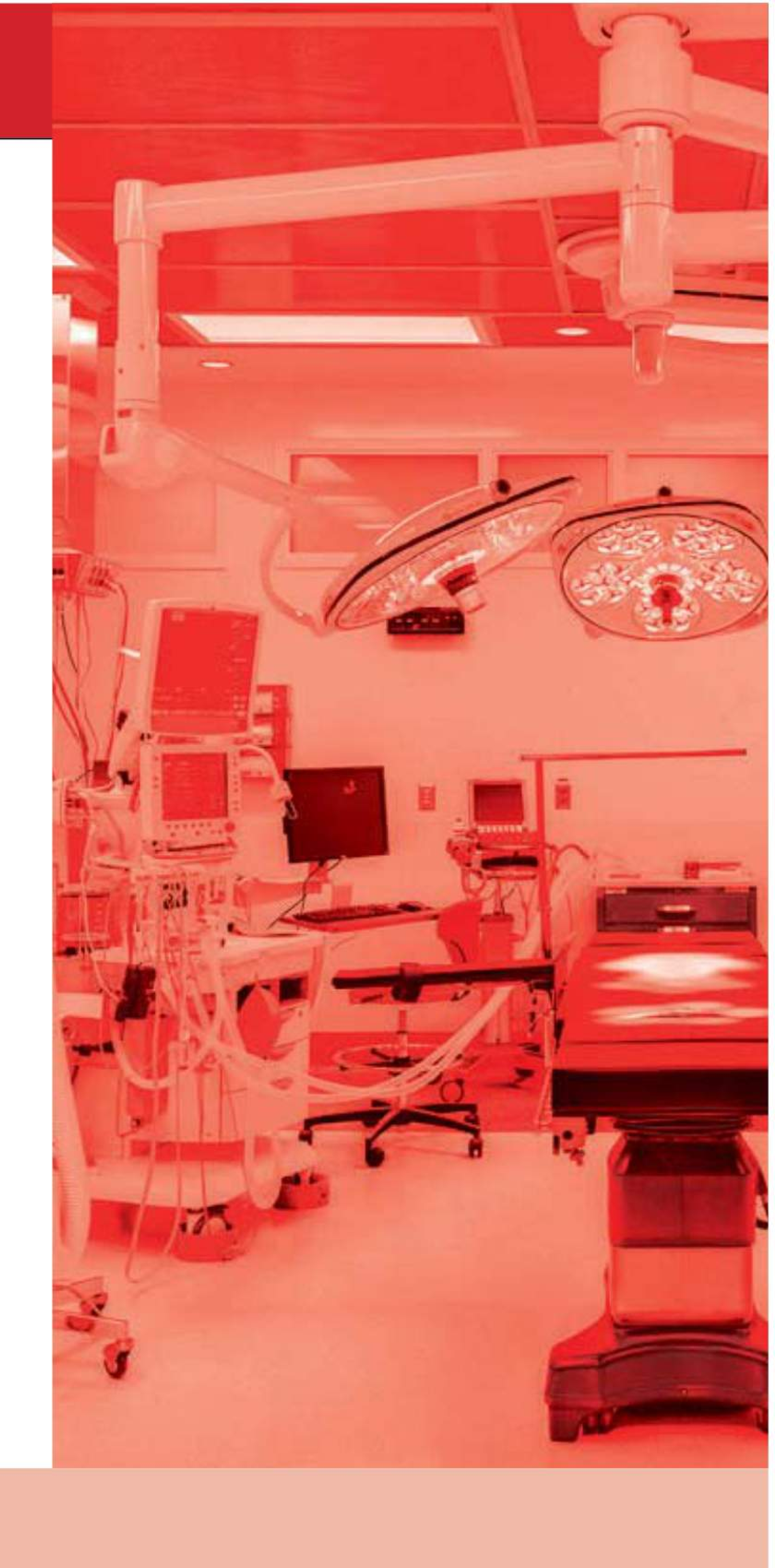
Según Kaspersky Lab, el conductor puede hacer muy poco para evitar sentirse como una marioneta dentro de un vehículo moderno. Señalan que lo mejor es llevar al coche a revisión de manera periódica para que chequeen el correcto funcionamiento de todos los elementos informáticos. En la actualidad, todas las marcas de automóviles trabajan en desarrollar sistemas de conexión 'blindados' de cara al exterior, para evitar posibles intrusiones de hackers.

GPS 'TRAIDORES'

Investigadores italianos descubrieron un fallo en los navegadores que usamos en nuestros coches.

La mayoría de estos dispositivos cuentan con un sistema que permite al fabricante enviar al usuario alertas en tiempo real como, por ejemplo, si hay un accidente o una calle cortada por obras. El protocolo de comunicaciones que utilizan carece de seguridad y cualquier hacker con el equipo y conocimientos adecuados podría mandar sus propias alertas falsas. El navegador las utilizaría para calcular nuevas rutas, eliminando otras alternativas... y terminaría dirigiendo al conductor por donde el ciberdelincuente quisiera.





DIAGNÓSTICO LETAL

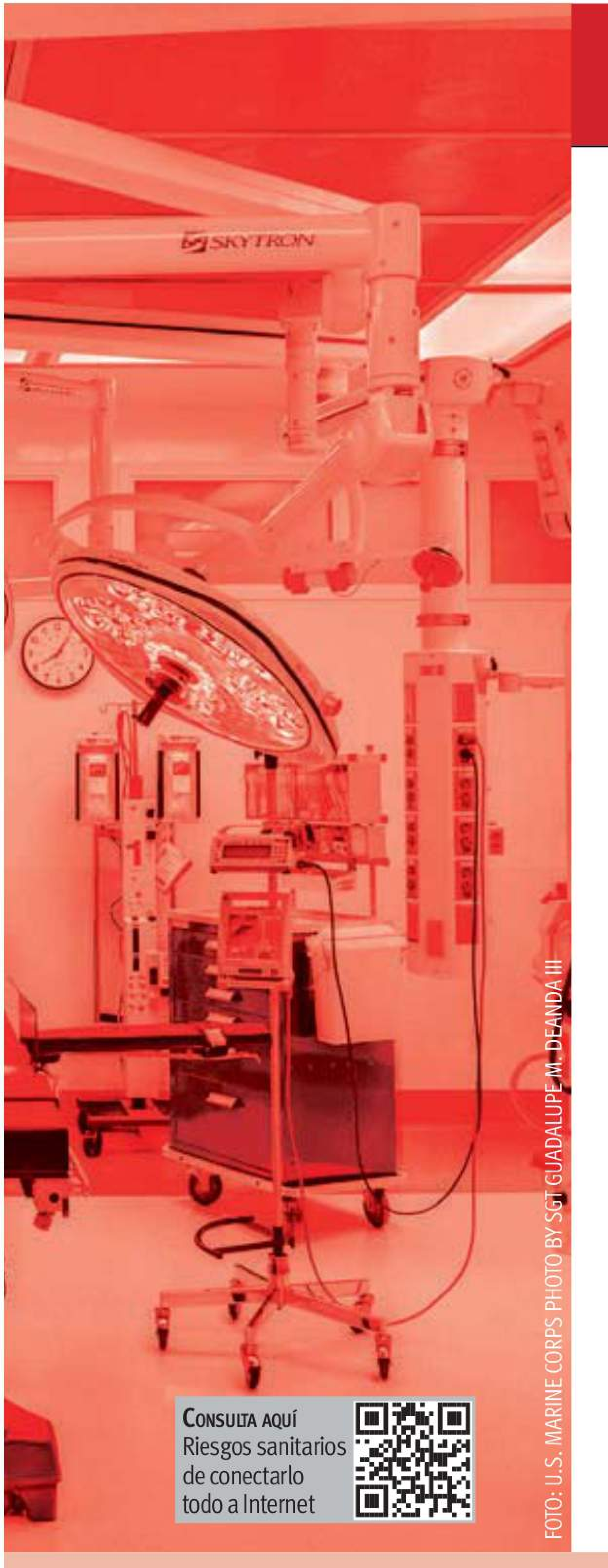
ASÍ PODRÍAN MATARTE... SI VAS AL HOSPITAL

Los hospitales son un quebradero de cabeza para la Seguridad Nacional. En ellos no sólo se reúne el mayor número de equipos radiactivos de cada país sino que, además, sus sistemas de diagnosis y tratamiento, dependientes de Internet, podrían ser fáciles de manipular por piratas informáticos que pretendan acabar con la vida de un paciente. // Texto: JJ. Altea

Si has visto la conocida serie de televisión estadounidense Homeland, ya sabrás que los aparatos con los que se diagnostica y se trata a los pacientes en los hospitales podrían ser vulnerables a los ataques de un hacker. En uno de los capítulos de la mencionada serie, el vicepresidente de Estados Unidos es asesinado cuando su marcapasos es 'ciberatacado' para que genere una descarga eléctrica letal. Según Chema Alonso, presidente de Eleven Paths -la filial de Telefónica especializada en seguridad informática- y uno de los mayores expertos en ciberseguridad de España, la situación que se muestra en Homeland es "realista", si bien la probabilidad de sufrir uno de estos ataques es baja porque muy pocos sabrían perpetrarlos.

El gran problema es que nadie se plantea dejar de usar Internet en estos aparatos porque supondría perder demasiadas funcionalidades, como la capacidad de adaptar sus funciones a cada paciente. "La buena noticia es que no tenemos conocimiento de ningún accidente en el mundo real. Pero la mala noticia es que no hay nadie científicamente interesado en estudiar el tema y evitar que algo así pueda suceder", explica el profesor de informática de la universidad de Michigan Kevin Fu, especializado en el ámbito de la salud.

Además, no sólo se pueden atacar los aparatos que se emplean para tratar a los pacientes: cuanto más débiles sean las contraseñas que los centros médicos usan para proteger las historias clínicas de los pacientes, más fácil será acceder a



CONSULTA AQUÍ
Riesgos sanitarios de conectarlo todo a Internet

FOTO: U.S. MARINE CORPS PHOTO BY SGT GUADALUPE M. DEANDA III

El hacker Barnaby Jack demostró, en varias convenciones públicas, que podía tomar el control de un marcapasos

ellas de forma remota. Cambiando los datos de los historiales, se puede inducir a los profesionales sanitarios a realizar diagnósticos erróneos, o a que administren medicamentos equivocados.

Por fortuna, hasta el momento no ha habido -o, al menos, no se han registrado- ciberataques contra hospitales o equipos médicos. De cualquier forma, se trata de un campo en el que se trabajará a medio y largo plazo, porque el empleo de un marcapasos, una bomba de insulina o un suministrador de medicamentos es algo sin lo que no se puede vivir.

DESFIBRILADORES

¿Qué son? Sirven para reanimar a una persona cuando ha sufrido una parada cardio-respiratoria. El desfibrilador se coloca sobre el pecho, y equipa unos sensores que analizan el ritmo cardíaco del paciente: si se estima conveniente, aplica una descarga eléctrica con la que se pueden corregir los trastornos que se aprecien en dicho ritmo.

¿Qué les pueden hacer? El profesor Fu ya advirtió, en un estudio de 2008, de los riesgos que suponían estos 'aparatos' implantados en el cuerpo humano, ya que los piratas pueden reprogramarlos infiltrándose en las redes inalámbricas que sirven para dirigirlos. Existen desfibriladores a los que se puede acceder vía Bluetooth, y que podrían ser manipulados por un hacker para aplicar descargas aleatorias al corazón de un paciente o conseguir que dejase de funcionar en el peor momento para su corazón.

MARCAPASOS

¿Qué son? Aparatos electrónicos que se implantan a aquellos pacientes cuyo corazón no puede mantener el ritmo cardíaco de forma natural. El marcapasos envía impulsos eléctricos para estimular el corazón artificialmente.

¿Qué les pueden hacer? El hacker Barnaby Jack demostró, en convenciones públicas, que era

CUATRO FORMAS DE 'COLARSE' EN LOS SISTEMAS DE UN HOSPITAL

01 Consiguiendo las contraseñas de sus equipos informáticos. "Muchos hospitales tienen equipos y ordenadores que utilizan contraseñas por defecto con un nivel de seguridad ínfimo como "Admin", "1234", "0000" explica un experto consultado por One Hacker.

02 Provocando que los empleados consulten webs falsas. Una de las maneras más habituales para hackear un ordenador es atraer a su usuario -en este caso, un empleado del hospital- a webs similares a las de conocidas compañías -pero falsas-, el llamado Phising, desde donde se descarga un virus informático para acceder a las redes del hospital.

03 Desde el propio hospital. Un delincuente que se encuentre en las dependencias hospitalarias también podría conectar su portátil a la red para descubrir y atacar sistemas vulnerables.

04 Hackeando un dispositivo conectado a Internet. Los fabricantes de dispositivos sanitarios trabajan a marchas forzadas para ofrecer la máxima ciberseguridad en aquellos productos radiológicos, de diagnóstico, de ultrasonido, robots quirúrgicos, etc.

05 Accediendo a las comunicaciones entre médicos. Muchos de los servicios en red utilizados en empresas y hospitales no disponen de comunicaciones encriptadas, por lo que la información procedente de los registros médicos se puede alterar. En caso de que un médico reciba una historia clínica podría aplicar un tratamiento letal a un paciente...

posible acceder a los marcapasos. Llegó a decir que podía matar a un hombre que se encontrara a nueve metros de él, simplemente accediendo a su marcapasos. La especialidad de Jack era dar con fallos de seguridad en los pequeños ordenadores con los que funcionan este tipo de 'aparatos' médicos. Sus trabajos provocaron tal revuelo, que el fabricante de dispositivos médicos Medtronic cambió el diseño de algunos de sus sistemas para protegerlos de intromisiones.

NEVERAS DE SANGRE

#**¿Qué son?** Frigoríficos diseñados expresamente para la conservación de la sangre procedente de donantes, pruebas médicas... Permiten regular la temperatura necesaria para mantener las muestras en el estado adecuado.

#**¿Qué les pueden hacer?** Se pueden alterar los parámetros de temperatura, mediante el robo de contraseñas y la introducción de virus informáticos.

TACS Y APARATOS DE RAYOS X

#**¿Qué son?** TAC son las siglas de 'tomografía axial computarizada'. Introduciendo al paciente en uno de estos aparatos, se pueden obtener imágenes del interior de su cuerpo. Los TACs usan rayos X, con los que se aplica una pequeña cantidad de radiación sobre la zona que se quiere observar del paciente. Gracias a los TACs se detectan tumores, lesiones internas, patologías en los huesos…

#**¿Qué les pueden hacer?** Se puede alterar la configuración de estos aparatos para exponer a los pacientes a cantidades de radiación más elevadas de lo tolerable. También se les puede causar daños que impidan o dificulten su uso. Eso sí, no son tareas fáciles para cualquier hacker: manipular estas máquinas requiere altos conocimientos médico-técnicos. En otras palabras, hay que conocerlos para saber qué puede variarse.

EQUIPOS DE ANESTESIA

#**¿Qué son?** Sirven para administrar de forma segura los gases y otras sustancias para dormir o calmar al paciente. Incluyen un ventilador con el que se ayuda a inspirar y espirar los gases a la persona que debe ser anestesiada. También cuentan hoy en día con procesadores que vigilan las constantes vitales del paciente.

#**¿Qué les pueden hacer?** Normalmente, los equipos de anestesia no están conectados a ninguna red informática. Pero los hackers sí que conseguirían acceder a ellos acoplándoles físicamente un ordenador con el que cambiar sus parámetros. De esta forma, podrían modificar las dosis de calmantes programadas.

BOMBA DE INSULINA

#**¿Qué es?** Un dispositivo que suministra insulina de forma continuada a los enfermos de diabetes. La insulina es una hormona que segrega el páncreas, necesaria para asimilar la glucosa, y que los diabéticos tienen problemas para producir. Una bomba de insulina se compone de un infusor -un microprocesador que se programa para administrarla durante las 24 horas del día- y el catéter a través del cual se introduce la dosis bajo la piel del paciente.

#**¿Qué les pueden hacer?** Al igual que sucede con el suministro de otras sustancias, los hackers pueden introducirse en el sistema y cambiar las cantidades establecidas. El exceso de insulina puede provocar hipoglucemia, que acarrea síntomas como dolores de cabeza, mareos, visión borrosa, cansancio…





RICARD MARTÍNEZ, presidente de la Asociación Profesional Española de la Privacidad -APEP-, colaboradora con asociaciones como AVISA, ISACA y SEIS.

¿ESTÁN SEGUROS TUS DATOS SANITARIOS?

01 Qué valor tienen nuestros datos sanitarios... Son cruciales tanto legal como materialmente y tienen una protección jurídica reforzada. El acceso y conocimiento por personas no autorizadas/adecuadas o su uso inadecuado de los mismos podría, por ejemplo, producir efectos discriminatorios desde un punto de vista social, para la contratación de un préstamo o seguro, o para el acceso al mundo laboral.

02 Cómo se protegen... En nuestra Ley son datos especialmente protegidos. Sólo pueden tratarse cuando una ley lo establezca o con consentimiento



expreso del paciente y siempre por profesionales sanitarios -que tienen el deber de secreto y confidencialidad-. Además, se exige un nivel de seguridad alto, lo que comporta especiales cautelas y deberes. Destacaremos uno: la trazabilidad. De cualquier cosa que se haga con un dato debe quedar rastro, debe saberse quién lo trató, cómo, y para qué. Además, la legislación exige consentimiento informado para su uso en la investigación, regula las condiciones de reidentificación en ensayos clínicos y, en un futuro inmediato, exigirá aplicar técnicas de análisis de riesgo de impacto en la privacidad para orientar cómo se usan estos datos en sistemas de información.

03 Cuál es el mayor riesgo que corren... Se ha especulado mucho con que los hospitales puedan ser objetivos estratégicos en caso de una ciberguerra. Las posibilidades criminales pueden ser tan variadas como la imaginación quiera y, para ello, basta con apuntar dos hipótesis: en la primera, sería posible falsear recetas para la dispensación de fármacos psicotrópicos, lo cual sería una clara actividad delictiva. En la segunda -si imaginamos un escenario extremo-, un delincuente podría paralizar un servicio esencial como la salud. Lo haría ralentizando la atención sanitaria, alterando historias clínicas y causando daños que provocarían una crisis parecida a la que se viviría en un estado de emergencia.

04 Qué pedís al nuevo Gobierno desde la APEP... Algo sencillo en su planteamiento y ambicioso en sus resultados: queremos concienciar a la comunidad sanitaria sobre el carácter estratégico que posee poner la privacidad y la seguridad del paciente, de sus datos, de su dignidad, en el centro del debate. La tutela de la privacidad y la seguridad de los datos no son una rémora ni en el ámbito asistencial ni en el investigador. Al contrario, permiten articular una sólida base de confianza mutua entre el sistema sanitario y los pacientes y contribuyen de modo significativo a la calidad de la atención sanitaria.



¿QUÉ SERVICIO EN

Dos de cada cinco ordenadores están infectados por virus que pueden destruir tus archivos. ¿Es la nube el lugar más seguro para guardar fotos, videos, información confidencial de una empresa...? Y, ¿qué debes tener en cuenta a la hora de elegir la tuya? //

Texto: Santy Torres

España ocupa el puesto 15 en la lista de países con mayor porcentaje de software malicioso -programas que se infiltran en sistemas informáticos para dañarlos-, según un estudio de la empresa de ciberseguridad Panda Labs. Y es que, en nuestro país, el 20% de los ordenadores están infectados o serán controlados por ciberdelincuentes en algún momento de su vida. Por eso, cada vez más empresas y particulares muestran mayor preocupación sobre cómo guardar sus archivos -imágenes, vídeos, documentos de contabilidad, etc.- de forma segura. Así, surge la nube -'cloud'-, un sistema que permite almacenar datos en línea, de forma que si tu ordenador o pendrive se ven infectados por algún virus, tus documentos se mantengan a salvo... porque no estarán físicamente en tu dispositivo, sino en un servidor de Internet, que cuenta con muchas más medidas de seguridad que cualquiera de los aparatos que utilices.

¿Cuál es el inconveniente? Una vez que envías los archivos a un sistema 'in cloud', la información deja de ser 100% tuya -también deja de estar bajo tu control total-, al ser administrada por un proveedor externo, como Dropbox, por ejemplo. Por ello, "lo más importante es averiguar cómo de en serio se toma el proveedor la seguridad, la confidencialidad y la salvaguarda de los datos de sus clientes", explica Óscar Maqueda, especialista de Microsoft para el sector público. Sus recomendaciones: leerse la política de uso y privacidad de estas herramientas para descubrir en qué país están los servidores 'cloud' de cada empresa.

¿BAJO QUÉ LEY ESTÁN ESTAS NUBES?

Todos estos servicios -salvo Mega- indican en sus políticas de privacidad que han aceptado el Safe Harbor. Se trata de una normativa -las empresas no están obligadas a firmarla, pero si lo hacen, deben cumplirla- para que las compañías de EE.UU. se acojan a unas medidas de seguridad y protección de datos fijadas por la Unión Europea, ante las que deben responder en caso de incumplimiento o de que se produzca algún incidente.

¿LEY EUROPEA O AMERICANA?

"Hay que fijarse bien bajo qué jurisdicción está ese servicio", recuerda Maqueda. Así, en caso de producirse un problema, las autoridades españolas tendrán una vía de actuación más sencilla si la empresa está sujeta a la legislación europea -porque tiene su sede en nuestro continente, como es el caso de Microsoft-, que si responde a normativas de Estados Unidos.

Asimismo, conviene asegurarse de que la 'cloud' en cuestión cumple con la ISO 27018, una



normativa sobre seguridad en la nube que prohíbe a los proveedores realizar data 'maining' -es decir, explorar los datos que guardan de la gente... con fines comerciales-: elaboración de estadísticas, creación de bases de datos, etc. "Los documentos no deben formar parte del negocio, deben ser siempre de los clientes", apostillan desde Microsoft.

QUÉ MEDIDAS DE SEGURIDAD DEBES TENER EN CUENTA

Para reforzar la seguridad en la nube, el arquitecto de seguridad de la compañía tecnológica Akamai, Michel Thomasius, aconseja activar siempre la conocida como doble autentificación que ofrecen algunos servicios, como Google Drive o OneDrive. Éstos, además de pedirte una contraseña cada vez que te registres para acceder a tus datos almacenados, te pedirán una clave adicional que te enviarán al móvil vía SMS. Todo con el fin de ponérselo un poco más difícil a los ciberdelincuentes que intenten acceder a tu información. Algo que no está de más, si tenemos en cuenta que, según un estudio de las empresas de ciberseguridad Kaspersky Lab y B2B International, sólo el 22% de los usuarios utiliza passwords diferentes para sus cuentas; el 20% las comparte con sus familiares y amigos; y el 9% guarda todas sus claves en un archivo... dentro del propio ordenador.

En el caso de las imágenes personales o documentos con información sensible de una empresa, la Oficina de Seguridad del Internauta -OSI- recomienda subir los datos a la nube una vez cifrados, con programas como Bitlocker, Folder Vault, My Lockbox o Secure Gallery. Así, los documentos serán invisibles para agentes externos y sólo podrán abrirse mediante una contraseña. Eso sí, la contraseña debe ser robusta -es decir, compleja- y no conviene escribirla en ningún documento. Para ello, existen gestores como KeePass, que las genera y almacena de forma automática.

MITO 1: LA NUBE ES LA SOLUCIÓN DEFINITIVA

La nube no es infalible y, como cualquier otro programa o dispositivo, también puede presentar fallos de seguridad. "Al igual que ocurre con los equipos tradicionales, la seguridad de los datos es el mayor riesgo", comenta Michel Thomasius. En este sentido, la nube no sustituye, de momento, a las clásicas medidas de seguridad, como el cifrado de archivos o la realización periódica de copias de seguridad.

OTRAS CLAVES PARA NO FALLAR

El arquitecto de seguridad de Akamai destaca la importancia de comprobar que la empresa de almacenamiento 'in cloud' ofrece sistemas de realización de backup -copias de seguridad de los archivos-, para poder recuperarlos en caso de que se produzca algún incidente con el servicio. Algunos sellos de auditores independientes, como los de la Alianza de Seguridad en la Nube -CSA-, certifican si un sistema está testado regularmente y si es capaz de responder ante una incidencia de forma rápida y eficaz. En nuestro país, existe una acreditación de la Agencia Española de Protección de Datos.



ANÁLISIS: ¿QUÉ SERVICIO ELEGIR?
PRECIOS Y ALMACENAMIENTO EN LA NUBE



GOOGLE DRIVE
BUENA INTEGRACIÓN CON MÓVILES

Esta herramienta permite almacenar, de forma fácil y gratuita, hasta 15 GB de fotos, vídeos, artículos, grabaciones de voz, archivos PhotoShop… Esta nube tiene muy buena conectividad -es fácil de utilizar- con diferentes dispositivos, desde PC y Mac, hasta sus respectivas apps en Android, iOS y Windows Phone. Además, Drive permite compartir un archivo con otras personas e, incluso, editarlo de forma simultánea. Así, por ejemplo, dos usuarios pueden trabajar a la vez en una misma hoja de Excel, aunque estén a miles de kilómetros. Por último, cuenta con un sistema de doble verificación.

■ **PRECIO:** Los 15 primeros GB son gratis. A partir de ahí, 100 GB de almacenamiento extra cuestan poco menos de 2 euros al mes y 1 TB -1000 MB-, unos 9 euros -alrededor de 100 al año-.

DROPBOX
PARA LOS ARCHIVOS MÁS PESADOS

Entre sus medidas de seguridad destaca la posibilidad de añadir el sistema de doble verificación. Además, mantiene una óptima conectividad con los smartphones, lo que permite descargar o ver cualquier archivo en múltiples dispositivos. Su gran ventaja respecto a otros servicios es que, aunque tiene menos capacidad inicial, no pone límites a la subida de archivos de pago -por ejemplo, OneDrive solo permite subir archivos de hasta 10 GB-.

■ **PRECIO:** La versión básica es gratuita, pero sólo ofrece 2 GB de capacidad. Existe una versión Pro, de 1 TB, por 9,99 euros al mes -cerca de 110 anuales-.

MITO 2: EE.UU. ESPÍA LAS CUENTAS DE LA GENTE

"Es ridículo pensar que la nube de Microsoft está vigilada por Estados Unidos, porque los servicios se dan bajo jurisprudencia europea", subraya Óscar Maqueda. En caso de que un proveedor 'cloud' facilitase información a un Estado, estaría infringiendo la Ley de Protección de Datos, al enviar información de un país a otro sin previo consentimiento de la parte afectada. Las sanciones, tipificadas como graves, podrían ir desde los 300.000 hasta los 600.000 euros. De hecho, "una policía estadounidense no puede inmiscuirse en el espacio europeo salvo sospecha de actividad terrorista", enfatiza el experto. Y, para hacerlo, necesitaría una orden judicial mediante los modelos de colaboración entre países.



iCLOUD
PARA LOS USUARIOS DE APPLE


Viene, de serie, en todas las tablets y teléfonos de Apple, por tanto también es muy práctica para los ordenadores Mac. Resulta especialmente útil para realizar copias de seguridad de las fotos del iPhone o para guardar una copia de estos archivos en el ordenador.

■ **PRECIO:** El usuario recibe 5 GB gratuitos al registrarse en el servicio, lo que equivale aproximadamente a unas 2.000 fotografías. Aumentar su capacidad en 50 GB cuesta 11,88 euros al año. Si se quieren conseguir 200 GB, el precio asciende a casi 36 euros y 120 euros si se desea contar con 1 TB.

ONEDRIVE
IDEAL PARA WINDOWS

No es la opción que más almacenamiento ofrece, pero es la alternativa económica para quienes no precisen de un gran volumen de espacio y quieran contar con la experiencia de Microsoft; además, funciona de maravilla en ordenadores que tienen instalado Windows 8 en adelante. Los móviles con Windows Phone incorporan, de serie, una versión de este sistema 'cloud', pero también existe una aplicación para iPhone y Android.

■ **PRECIO:** La nube de Microsoft







ofrece 15 GB de almacenamiento totalmente gratuitos. Aquellos usuarios que logren qu eotras personas se registren en OneDrive, recibirán 0,5 GB extra de regalo. Incrementar el límite hasta 100 GB supone un coste mensual de 1,99 euros -unos 24 euros al año- y 200 GB supondrían 3,99 euros al mes –cerca de 48 por año-.



MEGA
MUCHO ESPACIO SIN PAGAR

Cuenta con un sistema de almacenamiento de datos encriptado -algo que aporta más seguridad a la información que guardemos- y entre los planes de futuro de Mega está desarrollar una tecnología que lleve esa medida de seguridad a los correos electrónicos, las llamadas y las emisiones de vídeo.

▪ **PRECIO:** Es su gran ventaja: hasta 50 GB de almacenamiento gratuito para todos sus usuarios -el que más espacio inicial ofrece sin coste-. Asimismo, una versión Pro, con 4 TB, está disponible por 8,33 euros al mes. Es decir, apenas roza los 100 euros al año.

SUGARSYNC
OTRA ALTERNATIVA PARA MÓVILES

iPhones, iPads, Blackberry, Windows Phone, cualquier dispositivo con Android e, incluso, Symbiam son compatibles con este sistema en la nube. ¿Su principal limitación? La versión gratuita -que ofrece 5GB de almacenamiento- sólo está disponible durante un plazo de 90 días.

▪ **PRECIO:** Aparte de la mencionada versión sin coste, también ofrece planes de 100 GB –supone unos 90 euros al año-, 250 GB –cerca de 110 euros por un año-, 500 GB –sube a 290 euros- y hasta opciones personalizadas que permiten incrementar la cifra hasta varios TB –más de 500 euros al año-. Es, por lo tanto, una de las opciones más costosas.

MITO 3: LAS NUBES PRIVADAS SON MEJORES QUE LAS PÚBLICAS

Por regla general se puede hablar de cuatro tipos de sistemas 'cloud' o nubes:

▪ **LOS PÚBLICOS:** Aquí, un proveedor o compañía ofrece el servicio a los usuarios.

▪ **LOS PRIVADOS:** Una compañía adquiere un servidor y crea su propia nube para su uso exclusivo.

▪ **LOS HÍBRIDOS:** Una compañía vuelca en la nube pública los archivos que 'no le caben' en su nube privada.

▪ **LOS COMUNITARIOS:** Varias empresas, con interés común, ofrecen servicio a varias compañías del mismo sector.

Existe una cierta tendencia a creer que las nubes privadas se diseñan con mejores criterios de seguridad. Sin embargo, desde Microsoft, Maqueda no opina lo mismo. "Creo que no cuentan con todas las 'medidas escudo' que aplican las públicas". A su entender, las 'cloud' públicos dan servicio a miles de clientes, por lo que, lejos de lo que piensa mucha gente, precisan de sistemas de seguridad más avanzados.

En cualquier caso, al final todo depende de las necesidades de cada empresa. Desde Akamai Security, explican que algunas compañías prefieren los sistemas privados porque están creados específicamente para cumplir con los criterios deseados por el cliente. Es decir, son nubes 'a la carta'. "Son como centros de procesamiento de datos en los que la seguridad está directamente gestionada por el cliente", argumentan.



AMAZON CLOUD DRIVE
FOTOS SIN LÍMITES

La nube de Amazon no es de las más conocidas, pero destaca por su planteamiento revolucionario. Si un usuario decide hacerse miembro Premium -con un coste de 19,95 euros al año-, la plataforma le ofrece la posibilidad de subir todas las fotos que quiera a su nube sin que le suponga un cargo adicional.

▪ **PRECIO:** Respecto a sus tarifas básicas, Amazon ofrece 5 GB gratis para todos sus usuarios y ampliaciones que van desde los 20 GB -8€ al año- hasta 1 TB –por 400€ al año-. No es la opción más barata, pero sí es una opción muy atractiva para los que quieren la nube, sobre todo, para subir fotos.

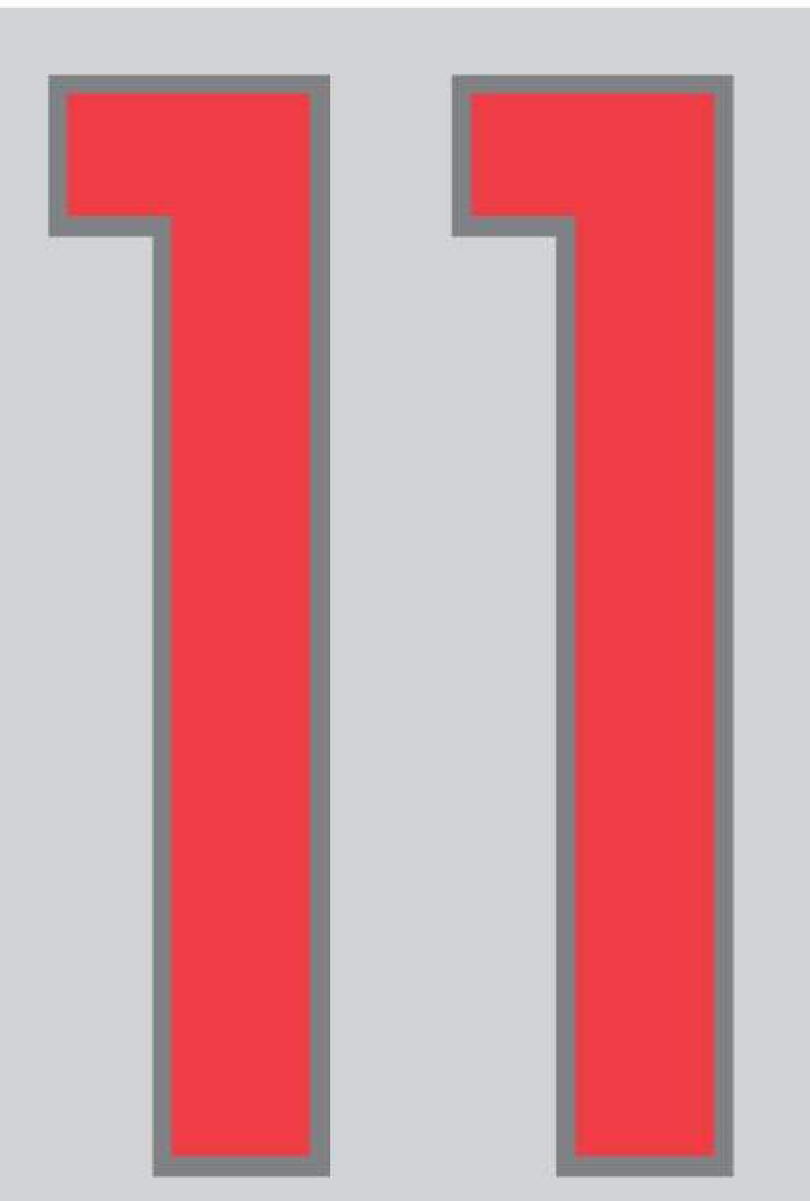


AZURE
UN COMPLETO PACK PARA EMPRESAS

Es la solución de Microsoft para las empresas que precisen de servicios en la nube más profesionales. En su web oficial, Azure asegura que firmas como EasyJet o la cadena NBC ya utilizan sus servicios. Además del clásico almacenamiento, este servicio 'cloud' permite crear aplicaciones virtuales, procesar datos... entre otras opciones. Es como tener un equipo con sus propios programas y sistemas pero creado en la nube.

▪ **PRECIO:** Son muy variados. Por ejemplo, 100 GB rondan los 120 euros al año, pero ofrece planes para cifras de hasta varios TB.





11 COSAS INCREÍBLES QUE VERÁS EN CYBERCAMP

Más de 7.000 personas asistirán a la segunda edición del que será el gran foro de ciberseguridad y búsqueda de talento: Cybercamp. Organizado por el Instituto Nacional de Ciberseguridad, en él podrás asistir a todo tipo de conferencias: desde las que explican cómo investiga una ciberextorsión la Policía Nacional, a través de su brigada tecnológica, hasta cómo se prepara España para la ciberguerra, gracias a los expertos del Mando de Ciberdefensa, o la forma en la que el Centro Criptológico Nacional -CCN-, del Centro Nacional de Inteligencia, protegen la red digital de ministerios, comunidades autónomas y ayuntamientos.

También habrá talleres prácticos, con diferentes niveles de dificultad, en los que se mostrarán herramientas de software para realizar test de seguridad para empresas, ver cómo trabajan los peritos forenses... Por supuesto no faltarán muchas nociones para convertir una Start-up en una gran empresa, a través del ejemplo de compañías como Panda Security y Vulnerabilidad. Como novedad, en esta edición se han incrementado las actividades para niños, incluyendo, incluso, obras de teatro inspiradas en el mundo de la seguridad informática, como 'Atrapada en la Red'.

CONFERENCIAS DE NIVEL

De los mejores hackers

■ Podrás disfrutar de conferencias de los expertos nacionales e internacionales más conocidos. Algunos de ellos, como Rubén Santamarta, de IoActive, explicarán cómo comenzaron en el mundo de la ciberseguridad hasta convertirse en una referencia... y cómo puedes hacerlo tú.

TALLERES PRÁCTICOS

Para expertos... y los que quieren serlo

■ **Novedades** Se hablará de nuevos campos de la seguridad en los que queda mucho que hacer. Por ejemplo, Pablo González y Rafa Sánchez abordarán la seguridad del próximo protocolo más usado en Internet -IPv6-. Y Friginal López y Miguel Martínez Raga explicarán cómo se protegen y cuáles son los puntos débiles de los sistemas informáticos de las infraestructuras críticas -con una 'demo' práctica-.

■ **Desarrolla tu software** Aprende a diseñar tu propia herramienta de ciberinteligencia. Deepak Daswani, del Deloitte CyberSOC Academy, que ha desarrollado su propio programa para conocer datos de personas a través del WhatsApp, te explicará qué hay que tener en cuenta.

■ **Dudas legales** Luis Jurado Cano explicará qué novedades tiene el nuevo Código Penal y la nueva Ley de Enjuiciamiento Criminal en su taller 'Malditos hippies de Internet'.

PARA GRANDES Y PEQUEÑOS

■ **Actividades** Los niños -deben tener 9 años o más- podrán participar en una competición sobre ciberseguridad en la que tendrán que superar todo tipo de retos, demostrando su cultura 'hacker'.

■ **Charlas** Disfrutarán de conferencias sobre cómo disfrutar de Internet de forma segura a través de divertidas historias, juegos, talleres musicales y obras de teatro.

■ **Talleres de tecnología** Habrá tres tipos de talleres en la zona de ocio: uno dedicado a robótica –en el que se podrán ensamblar robots-; otro sobre cómo integrar en nuestra ropa dispositivos inteligentes -wearables-; y un taller Lego para montarr piezas o crear robots con su tecnología Mindstorm.

■ **También para padres** Se impartirán charlas en las que se explicará cómo utilizar diferentes herramientas de control parental –para controlar la vida digital de sus hijos-, así como qué hacer en caso de ciberacoso. Teodoro Fernández Álvarez mostrará cómo configurar el nuevo Windows 10 para evitar problemas de seguridad.

5 HACKERS QUE NO TE PUEDES PERDER

En su segunda edición, el campus del Instituto Nacional de Ciberseguridad -INCIBE- volverá a ofrecer talleres informáticos para expertos, con los mejores hackers de todo el mundo, ofertas de empleo y, también, actividades para que los más pequeños se inicien en el mundo de la programación.

CONCURSOS Y RETOS

Demuestra que eres el mejor

■**Al límite** Se organizarán varios retos en los que los hackers competirán entre si. El más conocido será un hackton –término mezcla de hacker y maratón-: una prueba para desarrollar software por equipos con un tiempo limitado. Las grandes empresas presentes en Cybercamp siempre se fijan en los ganadores para contratarlos.

■**Premios** Se entregarán los premios de CyberOlympcis Games organizados por el Incibe entre institutos y colegios de toda España que han presentado trabajos sobre distintos campos de la seguridad.

LO ÚLTIMO EN TECNOLOGÍA

■**Realidad virtual** Podrás conocer a fondo esta tecnología y llevarte gratis unas gafas que te permitirán disfrutar de contenidos digitales en 360º.

■**Disfruta del futuro** Se mostrarán tecnologías increíbles como pantallas digitales –sin cristal- con las que puedes interactuar, demostraciones de cómo funcionan las impresoras 3D o cómo se crea un holograma.

PODRÁS ENCONTRAR TRABAJO

■**Foro empleo y talento.** Se impartirán diferentes conferencias en las que se darán los mejores consejos de los que ya han tenido éxito en el mundo de la ciberseguridad. Además, podrás aprender de ellos cómo perfilar una entrevista de trabajo.

■**No te pierdas** Javier Caparrós explicará qué hace falta para dedicarse a la seguridad informática. Laura Pereiro mostrará cómo utilizar LinkedIn para conseguir trabajo en este campo.

■**Muchas grandes empresas** aprovecharán el evento para captar talento y ofrecer puestos de trabajo a los mejores expertos informáticos.

SAMY KAMKAR



Conferencia: Ataques Blindsided. Una referencia mundial, es conocido por crear uno de los virus informáticos más propagados de la historia: el 'gusano' MySpace.

KEREN ELAZARI



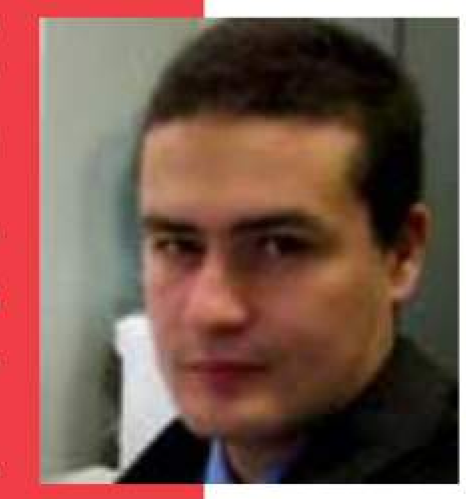
Conferencia: Hackea el futuro. Comenzó como una hacker aficionada y ahora es una eminencia mundial en divulgación en ciberseguridad con millones de seguidores.

DAVID BARROSO



Conferencia: Necesitamos OPSEC Uno de los españoles más activos a nivel internacional, con charlas sobre seguridad, ataques en redes, cibercrimen, etc.

ROMÁN RAMÍREZ



Conferencia: Riesgos de seguridad en el siglo XXI: familias y profesionales. Uno de los hacker españoles más populares y mediáticos, cofundador del congreso RootedCON.

YAIZA RUBIO

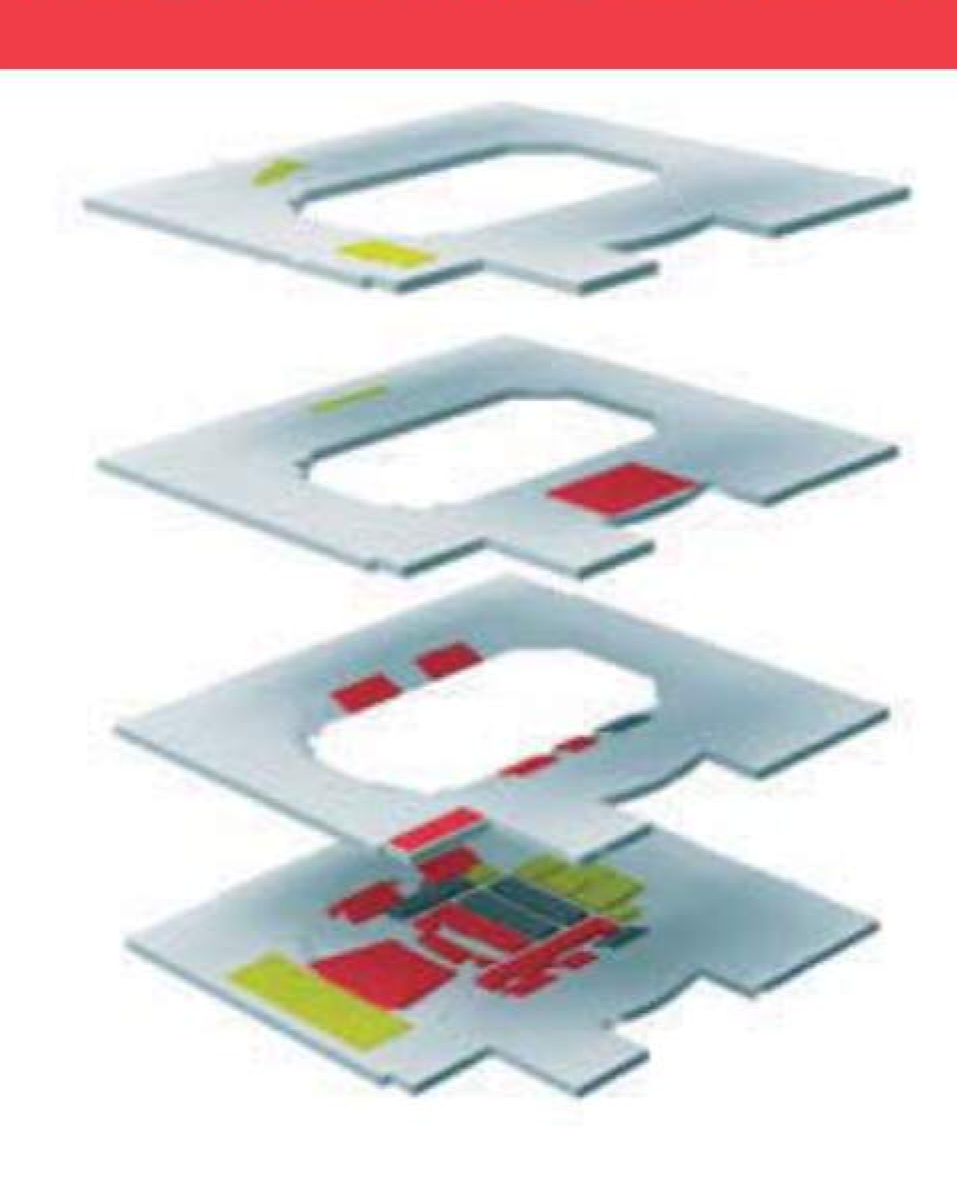


Conferencia: Big Brother is just one click away. Periodista y experta del Instituto de Ciencias Forenses de la UAM, es una de las mejores analistas de inteligencia en Telefónica Digital.

TAMBIÉN TE RECOMENDAMOS A: JOSEP ALBORS, DE ESET; JAVIER CANDAU, DEL CCN-CERT; RUBÉN SANTAMARTA, PEDRO CANDEL, FÉLIX BREZO, ALEJANDRO RAMOS...

TOMA NOTA...

■**Cuándo se celebra:** los días 27, 28 y 29 de noviembre. ■**Horario:** Viernes de 17 a 20 horas; sábado de 10 a 20 h. y domingo de 10 a 14 h. ■**Lugar:** En el Barclaycard Center -antiguo Palacio de los Deportes-, Avenida de Felipe II S/N, en Madrid. ■**Precio de la entrada:** Gratuita ■**Dónde apuntarse:** Hazlo en cybercamp.es/registrate ó en el propio evento. ■**Agenda:** www.cybercamp.es ■**Si no puedes asistir:** Síguelo en directo desde su web.



LA AGENDA HACKER

JORNADAS PARA PROFESORES "ESPACIO DE CIBERSEGURIDAD"

CUÁNDO 10 de diciembre de 2015, de 16:00 h a 21:00 h

DÓNDE Mallorca (Ubicación pendiente de confirmar)

ORGANIZADOR Incibe

QUÉ ES "Tienen como objetivo la capacitación como formadores de profesores de enseñanzas medias, de manera que adquieran las habilidades necesarias para impartir los talleres sobre ciberseguridad a sus alumnos".

REGISTRO espacioscs_profesores@incibe.es

IX JORNADAS STIC- CERT

CUÁNDO 10 y 11 de diciembre de 2015

DÓNDE Kinépolis, Ciudad de la Imagen, Madrid

ORGANIZADOR CCN - CERT

QUÉ ES "Ciberespionaje, APTs, cibercrimen, Internet de las Cosas, ENS y cumplimiento normativo, desactivación de infecciones, ataques a sistemas de pago o Smart Cities son algunos de los temas que se abordarán en estas Jornadas".

REGISTRO https://www.ccn-cert.cni.es

CONGRESO SECADMIN 2015

CUÁNDO 11 de diciembre de 2015

DÓNDE Avenida Reina Mercedes s/n 41012, Sevilla

ORGANIZADOR SecAdmin | Universidad de Sevilla

QUÉ ES "Combinan la administración de sistemas y la seguridad de la información compartiendo conocimiento útil y aplicable a sus entornos de trabajo y desarrollo profesional"

REGISTRO http://www.secadmin.es

SH3LLCON

CUÁNDO 22 y 23 de enero de 2016

DÓNDE Hotel Santemar, calle Joaquín Costa, 28, 39005, Santander

ORGANIZADOR SH3LLCON

QUÉ ES "Primer Congreso de Seguridad Informática en Cantabria. Foro de divulgación sobre seguridad informática que nace con la finalidad de analizar las distintas amenazas y vulnerabilidades que rodean nuestra conexión diaria en las redes. Si bien Internet es ya una parte más de nuestras vidas, aún existen aspectos desconocidos de nuestra actividad online".

REGISTRO http://www.sh3llcon.es

TEST ACADEMY

CUÁNDO 27 de enero de 2016

DÓNDE Berruguete, 126, 08035 Barcelona, España

ORGANIZADOR SH3LLCON

QUÉ ES "Es un día completo de varias 'master class' de una hora y media con expertos nacionales e internacionales del sector de las pruebas de software. Estas clases están orientadas a dotar a los testers de la información y de las técnicas necesarias para poder regresar al trabajo y aplicar el tema en sus actividades de pruebas del día a día".

REGISTRO http://www.expoqa.com/conference-inscripcion.php

III CONGRESO CIBERSEGURIDAD CANARIAS HACKRON

CUÁNDO 5 y 6 de febrero de 2016

DÓNDE Auditorio Caja Siete, Avda. Manuel Hermoso, 8. Santa Cruz de Tenerife

ORGANIZADOR Hackron

QUÉ ES El objetivo de Hackron con este congreso es "formar y aportar conocimientos en estas materias a las TIC y organismos oficiales de Canarias". Durante el congreso "todos los asistentes podrán participar en resolver el desafío de hacking: este año peligra la integridad de la primera fila de nuestro público, un sistema de misiles tele-dirigidos está siendo administrado por un sistema vulnerable". ¿Podrás evitarlo?

REGISTRO http://www.hackron.com

LLEVEMOS LA TEORÍA A LA PRÁCTICA. SI NO QUIERES QUE TU ORDENADOR ACABE INFECTADO O QUE TU RED WIFI QUEDE EN MANOS DE CIBERDELINCUENTES, PUEDES APRENDER CON LOS MEJORES EXPERTOS EN LAS JORNADAS SOBRE SEGURIDAD INFORMÁTICA QUE SE CELEBRAN CADA AÑO.

VIII FORO DE LA PRIVACIDAD

CUÁNDO 11 de febrero de 2016

DÓNDE CaixaForum, Madrid

ORGANIZADOR Data Privacy Institute

QUÉ ES "Uno de los encuentros de profesionales de la privacidad y la protección de datos más relevantes del Sector, en el que expertos, representantes de las autoridades de control y profesionales se dan cita para analizar y debatir sobre los nuevos retos que deberá afrontar el sector empresarial".

REGISTRO https://www.ismsforum.es/evento/data-privacy-institute

ROOTEDCON

CUÁNDO 3, 4 y 5 de marzo de 2016

DÓNDE Kinépolis, Ciudad de la Imagen, Madrid

ORGANIZADOR RootedCON

QUÉ ES Técnicas de intrusión informática, análisis de terminales móviles, peligros del cibersexo, funcionamiento del DNI electrónico, cifrado de contraseñas... Han sido sólo algunos de los muchos temas que vienen protagonizando este Congreso de Seguridad en los últimos años.

REGISTRO https://www.rootedcon.com

BLACK HAT USA

CUÁNDO del 30 de julio al 4 de agosto de 2016

DÓNDE Mandalay Bay, Las Vegas, Estados Unidos

ORGANIZADOR UBM Americas

QUÉ ES "Black HAT USA es uno de los eventos de seguridad de la información más importante y más técnico del mundo. Proporciona a los asistentes la última información sobre investigación de seguridad, desarrollo y tendencias. Este evento está impulsado por las necesidades de la comunidad de seguridad, empeñándose en reunir a las mejores mentes de la industria. Black Hat inspira a los profesionales de todos los niveles de carrera, instando al crecimiento y colaboración entre los académicos, investigadores de nivel mundial y líderes dentro de los sectores públicos y privado".

REGISTRO www.blackhat.com

CONGRESO&EXPO ASLAN

CUÁNDO 13 y 14 de abril de 2016

DÓNDE Palacio Municipal de Congresos de Madrid

ORGANIZADOR Asociación @asLAN

QUÉ ES "La tecnología es un pilar estratégico de esta imparable transformación que afecta a grandes y pequeñas organizaciones de todos los sectores. El Congreso y Expo asLAN 2016 pondrá el foco en esta revolución y el papel de la nuevas tecnologías". Big Data, Internet de la Cosas, Almacenamiento, Cloud, Virtualización, Centro de Datos...

REGISTRO http://www.congreso.aslan.es

SECURMÁTICA: CONGRESO GLOBAL DE CIBERSEGURIDAD, SEGURIDAD DE LA INFORMACIÓN Y PRIVACIDAD

CUÁNDO abril de 2016

DÓNDE Hotel Novotel del Campo de las Naciones, Madrid.

QUÉ ES La protección de la información laboral y personal así como la visión legal actual de la ciberseguridad son algunos de los ejes de estas jornadas organizadas por la revista SIC desde el año 1990. El evento reúne a universidades, bancos, cuerpos y fuerzas de seguridad... para organizar diferentes módulos de aprendizaje, a elegir según sus intereses.

REGISTRO http://www.securmatica.com

DEF CON

CUÁNDO del 6 al 9 de agosto de 2016

DÓNDE Paris/Bally's, Las Vegas, Estados Unidos

ORGANIZADOR Def Con. Fue creada por Jeff Moss, el mismo que hizo Black Hat

QUÉ ES "Es una de las convenciones de hackers más antigua y más grande del mundo"

REGISTRO https://www.defcon.org

www.onehacker.es

one Hacker

Directora Editorial Azucena Hernández
azucena.hernandez@grupoateneasn.es

Director adjunto One Hacker José M. Vera jose.vera@grupoateneasn.es
Subdirector Técnico Antonio Manzano antonio.manzano@grupoateneasn.es
Redactor jefe Javier García javier.garcia@grupoateneasn.es
Jefe de información Defensa David Noriega david.noriega@grupoateneasn.es
Jefe de internacional Borja García de Sola borja.garcia@grupoateneasn.es
Webmaster Sergio Álvarez sergio.alvarez@grupoateneasn.es
Creativa Elsa Ruiz elsa.ruiz@grupoateneasn.es
Colaboradores: Ana Pérez, Aurelio Valdés, Felipe Uemura, Enrique Checa, Sara G. Pacho, Laura Carretero, Santy Torres, Silvia Montes, Juanma Gallego, Rocío Sandoval, Elisa Coello, Emilio Pérez de Urigüen, Álvaro Marín, Alba García.
Colaboraciones especiales: Álvaro Sánchez, Ángel Tafalla, Antonio Núñez García-Sauco, Damián B. Jiménez, Federico Yáñiz, Fernando Sánchez Dragó, Emilio Pérez de Urigüen Muinelo, Ignacio Rupérez, J.A. Hernández, Joaquín Tamarit, Jorge Ortega, José Luis Bazán -corresponsal en Bruselas-, José Mª Blanco, José V. García, Juan Velarde, Manolo de Ramón, M. Ángel Benedicto, Mari Carmen Fuentes, Martín Hernández, Santiago Ávila, Santiago Gómez-Salgado. **Redes Sociales:** Raquel Sanelías.
Responsable producción/distribución: Teresa Brito teresa.brito@grupoateneasn.es

DISEÑO Jefe diseño Fernando Temprano fernando.temprano@grupoateneasn.es
Ayudante de diseño Leticia Machado Gundín leticia.machado@grupoateneasn.es
Fotografía Jotxo Cáceres / Nuria González / Teresa Brito

PUBLICIDAD Director Comercial y Márketing Andrés Hernández
andres.hernandez@grupoateneasn.es
Jefe de Publicidad nacional y Eventos Natalia Carrillo de Albornoz
natalia.carrillo@grupoateneasn.es
Jefe de Publicidad SN y Eventos Guillermo Moreno guillermo.moreno@grupoateneasn.es
Publicidad nacional e internac. y Eventos Pilar Lázaro pilar.lazaro@grupoateneasn.es
Publicidad SN y Eventos Pablo Díaz pablo.diaz@grupoateneasn.es



www.grupoateneasd.es
José Abascal, 18 - 1º
28003 Madrid (España)
Telf. 91 594 52 55 Fax: 91 448 80 95

Presidente y Director General José Luis Cortina

Director de Relaciones Institucionales y Director Adjunto al director
Pedro Díaz Osto
Secretario General Técnico Juan Antonio Pons

ÁREAS DEL GRUPO
Directora Editorial Azucena Hernández azucena.hernandez@grupoateneasn.es
Director General Comercial Andrés Hernández andres.hernandez@grupoateneasn.es
Director de Consultoría Francisco Serrano fserrano@grupoateneasd.es
Director de Eventos Ignacio Dancausa ignacio.dancausa@grupoateneasn.es
Director de Formación Valentín Martínez valentin.martinez@grupoateneasn.es
Administración Rocío de la Rubia administracion@i2v.es
Jefe de Informática Emilio Castellano emilio.castellano@grupoateneasn.es
Jefa de Secretaría Inmaculada Gómez inmaculada.gomez@grupoateneasn.es

Edita i2v SL (Grupo ATENEA) **Imprime** Einsa Print, Ctra. Cabanas – As Pontes s/n. Pol. Industrial de Penapurreira, CP 15328 As Pontes (A Coruña) **Distribuidora** SGEL, Avenida Valdelaparra, 29. 28108, Alcobendas, Madrid. **Transportes** BOYACA, Carretera M- 206 Km. 4.500 Loeches (Torrejón de Ardoz) 28890 Madrid.

Precio: 1,90 euros (IVA incluido), precio en Península, Baleares, Ceuta y Melilla -2,10 euros en Canarias-. Depósito legal M: 36541-2015

www.onehacker.es

